

THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL BUSINESSES

HEARING BEFORE THE COMMITTEE ON SMALL BUSINESS UNITED STATES HOUSE OF REPRESENTATIVES ONE HUNDRED FOURTEENTH CONGRESS FIRST SESSION

HEARING HELD
OCTOBER 7, 2015



Small Business Committee Document Number 114-024
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE

96-854

WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUTKEMEYER, Missouri
RICHARD HANNA, New York
TIM HUELSKAMP, Kansas
TOM RICE, South Carolina
CHRIS GIBSON, New York
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
CARLOS CURBELO, Florida
MIKE BOST, Illinois
CRESENT HARDY, Nevada
NYDIA VELÁZQUEZ, New York, *Ranking Member*
YVETTE CLARK, New York
JUDY CHU, California
JANICE HAHN, California
DONALD PAYNE, JR., New Jersey
GRACE MENG, New York
BRENDA LAWRENCE, Michigan
ALMA ADAMS, North Carolina
SETH MOULTON, Massachusetts
MARK TAKAI, Hawaii

KEVIN FITZPATRICK, *Staff Director*
STEPHEN DENIS, *Deputy Staff Director for Policy*
JAN OLIVER, *Deputy Staff Director for Operation*
BARRY PINELES, *Chief Counsel*
MICHAEL DAY, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

Hon. Steve Chabot	Page 1
Hon. Nydia Velázquez	2

WITNESSES

Ms. Stephanie Ericksen, Vice President, Risk Products, Visa Inc., Foster City, CA	4
Mr. Scott Everett Talbott, Senior Vice President, Government Affairs, ETA/ Electronic Transactions Association, Washington, DC	6
Mr. Paul Weston, President & CEO, TCM Bank, N.A., Tampa, FL	8
Ms. Jan N. Roche, President/CEO, State Department Federal Credit Union, Alexandria, VA, testifying on behalf of the National Association of Federal Credit Unions	10

APPENDIX

Prepared Statements:	
Ms. Stephanie Ericksen, Vice President, Risk Products, Visa Inc., Foster City, CA	33
Mr. Scott Everett Talbott, Senior Vice President, Government Affairs, ETA/ Electronic Transactions Association, Washington, DC	39
Mr. Paul Weston, President & CEO, TCM Bank, N.A., Tampa, FL	47
Ms. Jan N. Roche, President/CEO, State Department Federal Credit Union, Alexandria, VA, testifying on behalf of the National Association of Federal Credit Unions	52
Questions for the Record:	
None.	
Answers for the Record:	
None.	
Additional Material for the Record:	
American Bankers Association	67
The National Association of Convenience Stores (NACS)	75
The National Grocers Association (NGA)	83
The National Retail Federation (NRF)	88

THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL BUSINESSES

WEDNESDAY, OCTOBER 7, 2015

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 11:00 a.m., in Room 2360, Rayburn House Office Building. Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Luetkemeyer, Hanna, Rice, Gibson, Brat, Radewagen, Knight, Curbelo, Bost, Hardy, Kelly, Velázquez, Chu, Hahn, Payne, Meng, Lawrence, Takai, and Moulton.

Chairman CHABOT. Good morning. The Committee will come to order.

One week ago marked the official deadline for implementing the new EMV chip card technology. The shift away from traditional magnetic stripe credit cards to ones embedded with a chip adds an additional layer of security to every purchase, making our financial data less accessible to cyber criminals. The transition to EMV chip technology impacts every American consumer and is of great importance to this Committee. But just how much does the average American know about this transition? Many have probably received a new card in the mail, fewer have probably dipped their card into a new payment terminal, and many more may not know that a change is even taking place.

Given the number of electronic transactions that occur every day, this is a serious transition, and with it are some serious concerns. Small retailers are worried about the cost of implementing these new payment terminals, and then taking time to train staff on how to use them, and finally, helping consumers learn how to use them. And even though the technology shift was intended for October first, many credit card companies are still behind in issuing new cards to consumers. This poses significant challenges to sorting out liability issues in the case of cyber theft.

There are also questions about how much this actually does for security. For instance, when chip-enabled cards were introduced in the United Kingdom, fraudulent charges with counterfeit cards at the point of sale fell by 56 percent, but online fraud increased by 64 percent. These challenges are real, and they impact every American consumer and most small businesses.

Unfortunately, this transition seems to be catching many people off guard. A recent survey by the NFIB, the National Federation of Independent Business, found roughly half of small employers

who accept electronic payments were only somewhat familiar with EMV chip cards and a full 23 percent did not know anything about them at all.

Let me be clear. I did not convene this hearing today to take sides on this topic. This is a transition motivated by the private sector, not by any government regulation. And this Committee concerns itself with one thing, and that is the impact of this transition on small businesses. To fully understand that impact we must speak with all those involved. Today, we start by speaking with those who process our financial transactions. In a couple of weeks, we will speak with the small businesses and retailers who must purchase new payment terminals or risk being held liable for using old technology. We need to make sure everyone knows what is happening. The panel we have today, and those who will join us in our subsequent hearings will help us do that.

I want to thank the witnesses for joining us this morning to share their point of view on this transition and what it means for small businesses.

At this time, I recognize the ranking member for her opening statement.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Every day, millions of Americans use their credit cards and debit cards to make purchases. With increasing regularity, people are using them to buy everything, from candy to flat screen TVs, and even engagement rings. According to the Federal Reserve, card purchases now account for over \$4.8 trillion in consumer transactions annually, a twofold increase since 2007.

As consumer buying habits have moved toward the use of cards, merchants, especially small businesses, have had to follow suit if they want to stay competitive. We have all seen this progression. In just a few years, virtually every corner store and even vendors at farmer markets have become card-enabled. While the use of electronic payments has increased in the last decade, so, too, has point-of-sale fraud, which occurs when thieves steal the unencrypted account numbers stored on a card's magnetic strip.

Until recently, the U.S. was one of a handful of countries that still used magnetic strip cards exclusively. As a result, our country has been responsible for nearly half of all point-of-sale fraud globally, totaling \$6.4 billion, while accounting for less than a quarter of all transactions. In an effort to decrease such fraud, MasterCard and Visa set a deadline of October 1, 2015, for U.S. card issuers to replace magnetic strip cards with EMV cards and for merchants to begin accepting them.

EMV cards offer a significantly higher level of data security than stripe cards. Data on the chip is secure using both hardware and software security measures, so even if the card data is compromised, the chip itself will still be difficult to counterfeit.

While EMV is a step in the right direction that will lead to greater economic efficiency, implementation has been slow on both sides of the equation. Many financial institutions, and even more merchants are not yet in compliance, despite the announced transition being made over two years ago. In a troubling sign, millions of cards have now been replaced, and nearly one in two merchants has not upgraded their terminals to accept EMV cards.

In the many discussions I have had with stakeholders, the main barriers seem to be lack of awareness in the small business community, high costs to upgrade, and disagreements over verification methods. For small merchants, obtaining new terminals which range from \$50 to \$600 can be cost prohibitive in light of the amount of risk they face. For the deli or bakery owner, small day-to-day transactions are an unlikely target for thieves with stolen card numbers.

It is also an important distinction that EMV chips will protect against counterfeit cards but cannot eliminate fraud if it is lost or stolen. That is where authentication comes into play. Small merchants have raised concern regarding the financial industry's preference for signature verification over the use of a PIN.

As we all know, there have been outspoken proponents on both sides. Merchants have expressed the view that PIN is more secure, while financial firms have backed the signature method as just as secure and also more convenient.

I look forward to hearing about these issues. Regardless of which method is used, most observers, including the Federal Reserve Board, agree the chip cards will provide a more secure payment environment. Technological innovation holds great promise to spur economic activity.

EMV is not hack proof, but it is far safer than the magnetic strip status quo. As the first step in a move toward greater protection for our financial transactions, a smooth transition to EMV will lay the groundwork for new ways to secure our data, including biometrics. I look forward to hearing how the financial services industry is handling issues surrounding the EMV transition both in its own conversation as well as how they are assisting their small business clients.

And with that, I want to take this opportunity to thank all the witnesses for being here today.

Chairman CHABOT. Thank you very much.

If Committee members have opening statements, I would ask that they submit them for the record.

And I will take a moment to explain our timing rules here. It is basically the five minute rule. You all get five minutes to testify and then we get five minutes to ask questions, and there is even a lighting system. The green light will be on for about four minutes. The yellow light will come on letting you know you have about a minute to wrap up, and when the red light comes on, if you would not mind concluding your testimony then or close to then we would greatly appreciate it.

I would now like to introduce our distinguished panel here this morning. Our first witness is Stephanie Ericksen, vice president of Risk Products at Visa. Since joining Visa in 1994, she has been actively involved in developing the global smartcard implementation strategy. She is a graduate of the University of California-Los Angeles where she received a B.A. in History with specialization in Business Administration. She also holds an MBA in Marketing from Santa Clara University, and we welcome her here this morning.

Our next witness is Scott Talbott, who is the senior vice president for Government Affairs at the Electronic Transactions Asso-

ciation. He received his B.A. from Georgetown University, and his J.D. from George Mason University School of Law. We welcome you as well.

Our third witness this morning is Paul Weston. He has been president and CEO of Tampa Florida's TCM Bank since 2002. Today, TCM serves 200,000 cardholders and sponsors 640 community banks for competitive credit card services, in addition to providing ICBA member banks with payment card consultations. He graduated from Michigan State University, and completed the Graduate School of Retail Bank Management at the University of Virginia.

And I would now yield to our ranking member, Ms. Velázquez, for introduction of our next witness.

Ms. VELAZQUEZ. It is my pleasure to introduce Jan Roche. She is the president and CEO of State Department Federal Credit Union in Alexandria, Virginia. Jan has over 30 years of experience in financial credit union leadership. In addition to chairing the Community Depository Institutions Advisory Council for the Fifth District Federal Reserve Bank, she also serves as treasurer of the Credit Union Cherry Blossom 10-Mile Run here in D.C. Jan was elected to the NAFCU Board of Directors in 2013. Ms. Roche received her Bachelor of Science in Business Administration from the University of Richmond, and she is a certified public accountant in the Commonwealth of Virginia. Welcome.

Chairman CHABOT. Thank you very much.

Ms. Ericksen, you are recognized for five minutes.

STATEMENTS OF STEPHANIE ERICKSEN, VICE PRESIDENT, RISK PRODUCTS, VISA INC.; SCOTT EVERETT TALBOTT, SENIOR VICE PRESIDENT, GOVERNMENT AFFAIRS, ELECTRONIC TRANSACTIONS ASSOCIATION; PAUL WESTON, PRESIDENT AND CEO, TCM BANK, N.A.; JAN N. ROCHE, PRESIDENT/CEO, STATE DEPARTMENT FEDERAL CREDIT UNION

STATEMENT OF STEPHANIE ERICKSEN

Ms. ERICKSEN. Thank you. Thank you, Chairman Chabot, Ranking Member Velázquez, and members of the Committee. My name is Stephanie Ericksen, and I am vice president of Risk Products at Visa. Thank you for the invitation to discuss Visa's ongoing efforts to help transition the U.S. to EMV chip technology and what this means for small businesses. Given the current cyber threats, we need to move the payments industry away from static account information that can be stolen and used for fraud, to smarter, dynamic technologies that make payment data useless to criminals. Chip is an important part of this fundamental change in the payment system, and we are working to incentivize consumers and businesses to make the shift.

For those who are unfamiliar with chip cards, let me provide an overview of what they are and how they work. An EMV chip is a microprocessor that is embedded in a payment card or mobile phone. When a consumer uses a chip card at a terminal, a unique one-time code is generated, or cryptogram. This type of authentication adds a substantial layer of security and prevents cybercriminals from creating counterfeit cards. Counterfeit fraud

represents approximately two-thirds of the fraud that occurs in stores today, so as you can see, chip makes merchants less attractive targets for criminals.

In August 2011, Visa announced a roadmap to transition the U.S. to chip, and put in place a set of incentives to encourage adoption by financial institutions and merchants. A part of the incentive program, the party that has not implemented EMV by October 1st will be responsible for the loss from instore counterfeit fraud.

Getting the word out about this transition has been a key focus, and Visa has dedicated significant resources to raising awareness and providing small businesses with the tools they need and the information to adopt chip technology. In March, Visa launched our 20-city education tour to show small business owners how to demonstrate the value of chip. To date, we have traveled to 16 cities, including Cincinnati, New York, Miami, and Denver, to name a few, and more than 1,000 small business owners have turned out to learn about chip.

To amplify our efforts, we are closing working with other partners to provide critical resources to small businesses like the SBA, the NFIB, and local chambers of commerce across the country. Visa created a number of online resources, including visachip.com, which contains information specifically for the small business community. We have also worked with terminal providers to make transitioning to chip more easily accessible, especially to smaller merchants.

The cost of upgrading has been a key focus for us, and I want to highlight that low-cost chip terminal options are available for less than \$100, and in many cases, the terminal is included in the cost of the service. For example, Square recently announced a new \$49 reader that accepts EMV chip cards, as well as NFC mobile payments like Apple Pay and Samsung Pay.

This raises an important point for all of the mobile payment fans out there. When small business owners upgrade to chip-enabled NFC terminals, they are not just investing in payment and data security; they are also positioning themselves to accept the next generation of secure mobile payment technologies.

I want to emphasize that this is not a mandate. Visa's roadmap was designed with flexibility in mind, allowing businesses to make the transition on a timetable that meets their needs. In other words, October 1st marked the beginning of the process that will ultimately lead to near universal adoption of chip technology in the U.S., and we are pleased to report that great progress has already been made in this migration effort. Retailers, and particularly small businesses are making great strides. As of September 15th, more than 314,000 merchant locations are accepting EMV, which represents a 470 percent year-over-year increase. Just last month, roughly 50 percent of the \$4 billion in Visa chip transaction volume occurred at small businesses.

We are also seeing significant progress on the issuing side, with more than 150 million Visa chip cards in circulation in the U.S., up from roughly 20 million a year ago, making U.S. now the largest chip card market in the world.

It is important to note that while EMV eliminates instore counterfeit fraud, it does not prevent fraud in the online environment.

To help mitigate this, Visa developed technology called tokenization, which replaces the 16 digit account number with a unique digital token. When fully deployed, tokenization in combination with chip could virtually eliminate the need for small businesses to store cardholder account numbers.

Today, with the expertise gained from years working with merchants and financial institutions, Visa supports a wide variety of cardholder verification methods, including signature, PIN, and no-card verification for low-risk transactions, which represent over 60 percent of our transaction volume. However, we see dynamic verification technologies as the way forward, and I would like to share a few of these future technologies with you.

In February, Visa launched a new opt-in service that uses mobile geolocation information to reliably predict whether it is the account holder or an unauthorized user who is making a payment with a Visa account. In addition, last month, Visa introduced a new specification that can enable a range of biometrics in the authorization of payments, such as fingerprint or voice biometrics. This innovative technology is just rolling out but has great promise for protecting consumers in years to come.

There has been great progress in the past year in the U.S. transitions to EMV chip, but we must continue to work together to protect all stakeholders in the payment space, including small businesses.

Thank you for the opportunity to testify today, and I would be happy to answer any questions you may have.

Chairman CHABOT. Thank you very much.

Mr. Talbott, you are recognized for five minutes.

STATEMENT OF SCOTT EVERETT TALBOTT

Mr. TALBOTT. Thank you. Mr. Chairman, Ranking Member Velázquez, members of the Committee, I am Scott Talbott. I am senior vice president for Government Affairs at the Electronic Transactions Association, or ETA. Our member companies essentially represent all the major players and many of the minor players in the payment space. We focus on the acquiring side, which means we are the connection between the merchants and the payment system. So we are the handshake that helps make all these transactions possible.

This ecosystem and the payments ecosystem is one where the process is transacted securely and quickly, whether the consumer pays with a credit card, a debit card, a prepaid card; whether they tap, dip, swipe over the phone or over the Internet. And contextually, 70 percent of all consumer spending is done electronically. Last year, electronic payments totaled over \$5 trillion, with a "T". By 2017, we project that ETA members will process over \$7 trillion in electronic payments.

Combating fraud is a major focus for ETA members, and our payment system is built to detect and prevent fraud and to insulate consumers from liability. It is important to note that both before and after this EMV transition, consumers will enjoy zero liability for any fraud when using electronic payments.

Billions of dollars of fraud occur each year, and the largest category is counterfeit fraud. This is where a thief steals your active

account number, makes a fake card, and goes and uses it instore. Chip cards work to prevent this fraud by creating a special dynamic one-time code that runs with each transaction. So frauds who obtain a chip card account number will not know what this code is, and therefore, cannot create a counterfeit card to be used in stores.

As Stephanie mentioned to incentivize the industry to migrate to chip, last week, October 1st, the networks implemented a voluntary long-planned liability shift for payment card transactions. Liability shift means any participant, whether it is a bank or a merchant, who is not chip compliant, could be responsible for instore counterfeit fraud.

To make the switch, chip cards require the cooperation of eight million banks and credit union who have to issue 1.2 billion cards in the U.S., eight million or so merchants who are going to upgrade their equipment, as well as consumers are going to have to switch from the familiar swipe to a dip.

Small businesses across the board are beginning to become EMV compliant, and I would like to talk about the way they think about this process. First is the cost. The cost of upgrading one chip terminal is around at least \$50. I brought an example of one here today. CardFlight based in New York offers it for about \$50. The cost for each merchant depends on the complexity of their system. If they have multiple terminals, or if they have integrated terminals, the cost is going to be much higher, but on average it is going to cost about \$100.

So each merchant will have a different risk of fraud. They have a different fraud threat matrix, and it will compare this fraud threat matrix that they have to the cost of the upgrade, and those merchants who experience a lot of counterfeit card fraud because they sell easily marketable goods and services, like jewelry or electronics, they are more likely to be chip compliant, and if they are not, they will be quickly.

Those merchants that sell services and less marketable goods, like hotels or car washes or dry cleaners, are less likely to be complaint at this point. They may delay their decision to convert.

Once a decision to switch to chip cards is made, the merchant will work with their processors and other entities to get their terminal certified. This is essentially a quick audit that is done. For one terminal it is relatively simple, but if you have a complex number of terminals, it could take longer to become certified. And many processors are working with merchants who, if they requested to be certified before October 1, the start of the transition, if they are not complaint now, then the processor will actually cover the fraud for that particular merchant while they work to get them compliant.

To assist small businesses with the migration to chip, the payments industry is working with a large number of programs, both financial incentives, as well as educationally, both at the small business as well as at consumers. ETA, for example, has an educational website, sellsafeinfo.org, which is aimed at helping small businesses, and we will continue to work with them through the process. We are also working with state AGs and state regulators to help get the message out to consumers.

As I said earlier, chip cards only protect against instore counterfeit. They do not protect against online fraud. As we know from our experiences in Europe and Canada, the fraudsters will simply shift their focus from counterfeit cards to online fraud. To address online fraud, the industry is deploying another technology called tokenization. Tokenization essentially replaces the payment card information with a unique identifier that cannot be reversed. Another layer of protection that is being deployed by ETA members is point-to-point encryption. With point-to-point encryption, the data is encrypted during the transition process as the information runs across the systems and merchants or thieves cannot grab the information and use it to make fake cards.

So in conclusion, ETA members are the first line of defense against fraud and we take this very seriously, and every day we deploy a number of technologies—chip, tokenization, encryption, biometrics, and other technologies to help protect consumers, merchants, as well as the payment system from fraud.

Thank you for the opportunity to testify. I look forward to your questions.

Chairman CHABOT. Thank you very much.

Mr. Weston, you are recognized for five minutes.

STATEMENT OF PAUL WESTON

Mr. WESTON. Chairman Chabot, Ranking Member Velázquez, members of the Committee, my name is Paul Weston, and I am president and CEO of TCM Bank in Tampa, Florida. I testify today on behalf of more than 6,000 community banks represented by the Independent Community Bankers of America. Thank you for convening today's hearing.

TCM is a \$180 million credit card bank. We issue and service credit cards to 200,000 consumer and small business customers for 650 community banks across the country. We adhere to the values and standards of service of our community bank clients, and by functioning as their back office for credit cards, we allow community banks to focus on their core competencies, small business consumer, and farm lending. Community banks are uniquely positioned to help their small business customers make a smooth transition to EMV and are committed to doing so.

EMV, or chip cards, are much more secure than magnetic stripe cards because they are significantly more difficult to counterfeit. Counterfeit cards made with stolen information represent the largest portion of payment card fraud in the U.S.

While consumers are protected against loss, having to replace a credit card or a debit card is inconvenient for them at best. EMV, together with merchant-provided chip readers at the point of sale will play a critical role in reducing counterfeit fraud. Community banks are joining other financial institutions in the orderly migration to deploy EMV chip technology for debit and credit cards. Recent reports indicate that roughly 4 in 10 consumers already have an EMV credit card.

There is no mandate that card issuers adopt EMV or that retailers invest in EMV chip card readers. However, new card industry rules that took effect on October 1st incentivize a shift to EMV technology. The new rules provide that the liability for fraudulent

transactions sits with the party, the retailer, or the issuing bank that has not upgraded to chip technology, where neither party is yet EMV compliant or where both parties have upgraded, the pre-October 1 liability rules prevail. That is to say that the issuing bank is responsible for fraud losses.

October 1st is not a deadline in a meaningful sense of the word. Instead, the liability shift serves as a catalyst for change. Already, many card issuers in many merchant locations have enabled EMV. Others will adopt it before year-end, and some will choose to defer it until 2016 or even beyond. Each issuing bank and each merchant will decide when to adopt EMV based on their own business model, their vulnerability to fraud, and their management of risk. We expect the migration to full EMV chip card usage to take several years.

Based on many conversations with community banks and their small business customers, I believe that most small businesses are taking a very prudent approach to this migration. They are not buying from the first terminal salesman that makes the phone call, but they are planning to closely follow as the larger national retailers in their marketplace begin to enable EMV at the point of sale.

Community banks will serve as an important ally and resource to retail small businesses making this transition. They will help their merchant customers by providing equipment, expertise, and education to guide them through the change. Since community banks are local, they serve as the “feet on the street,” especially for the small businesses in their communities.

While EMV chip cards are an effective means of reducing fraud related to counterfeit, they are not a panacea for all types of payment card fraud. Multiple layers of security are needed in addition to EMV to mitigate the other types of fraud. End-to-end encryption should be deployed to protect cardholder information in transit, and newer technologies, such as tokenization, should and will be developed and deployed to protect online transactions.

Some are insisting that PIN technology in combination with EMV is the only way to eliminate payments fraud, but PINs only protect against fraud in cases of lost or stolen cards, which is a relatively small portion of total fraud. What is more, as a static data element, the PIN is more vulnerable to compromise than active technologies like EMV or tokenization.

The most important thing for cardholders to know is that they are fully protected from fraud losses as all the major credit card brands have zero liability provisions for consumers and small businesses. The Electronic Funds Transfer Act limits consumer liability for fraud on debit cards. Customers should also know that banks are subject to rigorous examination and supervision of their data security policies and procedures. We believe that similar standards should apply to all industries that handle sensitive customer financial information.

In conclusion, I fully expect that the critical partnership between local community banks and their small business customers will help ensure a smooth transition to EMV and a more secure environment for all payment card users.

Thank you again for the opportunity to testify today, and I look forward to your questions.

Chairman CHABOT. Thank you very much.
Ms. Roche, you are recognized for five minutes.

STATEMENT OF JAN N. ROCHE

Ms. ROCHE. Good morning, Chairman Chabot, Ranking Member Velázquez, and members of the Committee. My name is Jan Roche, and I am testifying today on behalf of NAFCU. I serve as the president and CEO of the State Department Federal Credit Union.

NAFCU appreciates the opportunity to appear before you today to discuss EMV. Due to the traveling habits and job assignments of many of our members, State Department Federal Credit Union was one of the first financial institutions in the U.S. to start issuing EMV credit cards. Today, our credit card portfolio of over 28,000 cards is now 100 percent EMV enabled.

EMV is the established worldwide standard for chip cards. EMV cards are still plastic but they contain an embedded microchip that makes it harder to produce a counterfeit card that can be used at a point-of-sale terminal. This is because the chip generates a new random number identifier for each transaction. If that data is stolen, it is not traceable back to the account. It is the EMV chip technology that makes the new cards more secure, not a PIN or signature. While EMV is the new market standard for combatting fraud at the point of sale and assigning liability when a fraudulent credit card is used, it is not a silver bullet solution to the broader problem of data security. Also, a chip card can only be effective if the point of sale terminal is configured to accept it.

It is important to note that the EMV transition in the U.S. is a voluntary one established by the market, and not a government mandate. Neither financial institutions, nor merchants, have been forced to transition. The speed of shifting to EMV is essentially a business decision that is dependent upon risk tolerance. Consumers are not liable for fraud losses in general. All credit cards have zero liability provisions for consumers and consumer liability is limited for any fraud on debit cards. This is true whether or not a card or business is EMV enabled.

NAFCU has found that a majority of credit unions are transitioning quickly and effectively to EMV. Even prior to the announced shift in liability, many were already providing EMV credit cards to their members as they issued new cards or replaced older magnetic stripe cards. This is true even though there is a greater cost for EMV cards at credit unions. At State Department Federal Credit Union, our cost for producing an EMV card is nearly double a non-EMV card.

A truly secure payment system must be one that evolves to meet emerging threats and utilizes a wide range of authentication technologies—EMV, tokenization, encryption, biometrics, and more. There is no panacea to avoid data theft.

Accordingly, NAFCU does not support any single solution, such as a PIN mandate, to require consumers to enter PINs for every transaction. A PIN is a static data element that is still vulnerable to theft. A PIN mandate would not have helped prevent recent consumer data breaches, such as Target, Home Depot, or Michaels.

Requiring PINs would not prevent online or mobile fraud, often referred to as “card not present” fraud. This type of fraud is also

expected to rise significantly after the EMV transition, as it has in other countries after their EMV transitions. For my credit union, “card not present” fraud was about 40 percent of our gross fraud this past year.

NAFCU has long supported comprehensive data and cybersecurity measures to protect consumer sensitive data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 Gramm-Leach-Bliley Act. Unfortunately, there is no similar regulatory structure for other entities that may handle sensitive personal and financial data. GLBA requires financial institutions to address the risks presented by the complexity and scope of their business. This allows flexibility and ensures the regulatory framework is workable for both the largest and smallest financial institutions. Gramm-Leach-Bliley is an example of how scalability is achievable for varying sized businesses.

In conclusion, a truly secure payment system must be one that is constantly evolving to meet emerging threats and uses a wide range of dynamic authentication technologies—EMV, tokenization, encryption, biometrics, and more. When it comes to EMV, what matters most is the chip technology that makes the cards more secure. Requiring additional measures, such as PIN usage does not make substantial improvements to the system. NAFCU encourages you to support H.R. 2205, the Data Security Act of 2015. This bipartisan legislation creates a national data security standard that is flexible and scalable. Ultimately, consumers will only be protected when every sector of the industry is subject to strong federal data security standards that are enforced by corresponding regulatory agencies.

Thank you for the opportunity to appear before you today. On behalf of NAFCU, I welcome any questions you may have.

Chairman CHABOT. Thank you.

I recognize ourselves to ask questions, and I will recognize myself first for five minutes.

Today is October 7th. The deadline for transition to this new technology is about a week old now. And I am going to have a little audience participation here. Just by a show of hands, how many in the audience used a credit card to purchase something over the last week? If we could just see a show of hands. Virtually, everybody in the room. I am not going to ask you what you purchased, but how many of you, if you know, used this new chip technology? Okay, quite a few. Excellent. Well, I appreciate that very much.

I know my staff could not use the new chip technology when they tried to do so in the cafeteria downstairs in this building this week, so that is something we probably need to work on. And we have had a similar shift before from paper processing to electronic processing. So we have experienced this to some degree before, and that certainly seems to have caught on, although I generally use cash myself.

So my first question is, and I will ask you, Ms. Ericksen, how is the transition going? I know it is still very early in the process, but how is it going?

Ms. ERICKSEN. Thank you, Mr. Chairman.

So we know from other countries that have moved to chip technology, it typically takes about two or three years after the liability

shift date to get to roughly 60 or 70 percent of a company's domestic payment volume being a chip card used at a chip terminal. So we are in very good shape in terms of being that we are really at the starting point of moving the west towards using this technology more frequently. And it typically takes about four or five years after the liability shift date to get to greater than 90 percent of the payment volume being chip-on-chip, or chip authenticated, if you will. So the fact that we already have more cards here in the U.S., more chip cards here in the U.S. than any other country, and great participation, particularly from many of the major retailers that even just turned on on Friday and Saturday last week, we are seeing increasing growth on the payment volume side of things.

If you look at consumers, many consumers have at least one card in their wallet; many of them have more than that. What we have seen from our research as of July is roughly 60 percent of consumers have at least one chip card in their wallet, and as of that time in July, 30 percent of them had done at least one chip transaction. But we know that many retailers just enabled in August and September, and many are enabling this month as well, so we are seeing that increase almost on a daily basis in terms of the actual penetration of people doing a chip transaction going forward.

Chairman CHABOT. Thank you. Let me ask you another question. The shift to payment cards with computer chips has happened, as we know, in other places all around the world, including Europe where the technology has been used for about 20 years now. What has the impact on fraud rates been in Europe specifically since the implementation of the EMV chip card? And what effect do you think that chip and PIN has had on instances of fraud in Europe? And what does that mean for the implementation here in the U.S.? What additional levels of security are financial service providers working on to better protect businesses and consumers and strengthen data security?

Ms. ERICKSEN. Yeah. Unfortunately, Visa Europe is a separate legal entity from Visa Inc., so I can speak to other parts of the world that have moved to chip technology around the same time and same pace compared to Europe.

Chairman CHABOT. Who would we need to go to to get the information?

Ms. ERICKSEN. Someone from Visa Europe or someone from Europe.

Chairman CHABOT. Can you recommend anybody on that?

Ms. ERICKSEN. We can get back to you on that for sure.

Chairman CHABOT. Okay. I would appreciate that very much.

Ms. ERICKSEN. We do have data to share though from other countries if you would like to hear that, from Australia, Brazil, and Canada.

Chairman CHABOT. I will get that later, but I have got a minute and 18 seconds left.

Ms. ERICKSEN. Okay.

Chairman CHABOT. A whole lot of questions, so

I understand that the cost is a deterrent to small businesses as we know, as well as training the employees to use the new system and even educating customers about how to use the new terminals, and these appear to be hurdles for small businesses, and this Com-

mittee is the Small Business Committee, so we are obviously very concerned about the impact this will have on small businesses. How are small businesses supposed to overcome some of these obstacles? And what are some of the challenges that they face? Are financial service providers offering any assistance to businesses that encounter these problems?

Mr. Talbott?

Mr. TALBOTT. Thank you. Good question. I think many financial institutions, as well as other entities like processors, are offering both financial incentives. American Express, for example, set aside \$100 million to help in this process. Other companies are providing low costs. For example, this CardFlight, this is \$50 attached to the merchant's phone to go on the low end. But there are lots of financial incentives, as well as educational incentives. There are videos, there are instore demonstrations, there is teleconferencing. The payments industry is working very hard to help the small merchant get to this process. The end result is to protect everybody themselves as well as consumers from fraud, and that is the ultimate goal.

Chairman CHABOT. Thank you very much. My time is expired.

I will recognize the ranking member, Ms. Velázquez, for five minutes.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Ms. Roche, as we know, under the new EMV agreements, liability to reimburse consumers for fraud loss shifts to the party that has not upgraded to EMV technology. What is the process for making consumers whole, and do they contact their bank like they have in the past? What is the process?

Ms. ROCHE. So the process will not change. The consumers, if they have noticed a fraudulent transaction on their account, they will contact their bank or credit union, whoever issued the card. And then my credit union specifically will reimburse the consumer, give them provisional credit, and then we will work it out on the back end as far as whether or not we recover those funds from a merchant.

Ms. VELÁZQUEZ. Thank you.

Ms. Ericksen, small businesses pay considerable sums of money to accept payment cards. Reasons given for these fees have often included the cost of fraud. If EMV successfully reduces fraud, will Visa commit to reducing swipe fees on its cards commensurate with that fraud reduction?

Ms. ERICKSEN. Well, our interchange rates that we have set are consistent across the industry in terms of incentivizing participation for issuers to issue cards as well as merchants to accept payments.

Ms. VELÁZQUEZ. But hasn't one of the arguments always been the cost of fraud?

Ms. ERICKSEN. Fraud is one component of it, including the credit risk of lending that credit to the cardholders.

Ms. VELÁZQUEZ. So how would you factor in if we see that there is a reduction in fraud, how will that—

Ms. ERICKSEN. Yes. Well, unfortunately, the criminals continue to invest in strategies in being able to commit fraud as well, so we need to continue to invest in the ability to address that fraud. So

even though EMV is one technology that is going to help drive fraud down, we need to continue to invest in analytics and other types of authentication technologies that continue to stay one step ahead of the criminals, because, unfortunately, they are going to continue to try to do that as well.

Ms. VELAZQUEZ. I just cannot help myself but laugh.

Ms. ERICKSEN. I am sorry, what is your question?

Ms. VELAZQUEZ. There is also typically two tiers of interchange fees for instore and online transactions.

Ms. ERICKSEN. Excuse me. We are not sure what the question is.

Ms. VELAZQUEZ. No, it is a statement.

Ms. ERICKSEN. Oh, okay.

Ms. VELAZQUEZ. Yeah. Will there be a day when we see a reduction? Also, in terms of Europe, you will provide Mr. Chabot the information on whether the percentage of fraud has gone down, correct?

Ms. ERICKSEN. The only statement that I have is the interchange fees that we have are very competitive, and they incentivize participation from both issuers and merchants to participate in accepting electronic payments, and we continue to invest in security and technologies to make that convenient, as well as to continue to provide consumers confidence in using electronic payments.

Ms. VELAZQUEZ. Mr. Talbott, thank you. In Europe where the EMV chips have been in use for decades, point-of-sale fraud is virtually nonexistent. What took so long for the standard to be implemented here in the U.S.?

Mr. TALBOTT. It is two different systems. Probably a better way to answer the question is, why was Europe implemented to quickly? And the answer is they did not have continuous access to the Internet that we do. So in Europe when a card was presented, the merchant needed a way to verify that transaction at that point since they would have to batch their transactions for authorization later that day when they could access the Internet. And the chip helped them do that, to verify the card at that point. They could not do it later when they went for authorization because the customer was gone. The U.S., by contrast, has always enjoyed continuous access to the Internet and the ability for merchants to process and gain authorization of that transaction in a couple seconds. And so there was less of a need for other authentication methods at the point of sale, which is why the U.S. is now and soon will be aligned with the U.S.

One other quick point, as we look at other technologies like tokenization and encryption, the U.S. is far ahead of Europe and other countries in developing and implementing those. And so these things do not move exactly lock step. It is sort of a cat and mouse type of approach.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

Chairman CHABOT. The gentlelady yields back.

The gentleman from Nevada, Mr. Hardy, who is chairman of the Subcommittee on Investigations, Oversight, and Regulations is recognized for five minutes.

Mr. HARDY. Thank you, Mr. Chairman.

Ms. Roche, I would like to start with you. In your testimony you mentioned that the largest consumer data breaches that happened in places like Target and Home Depot would not have been averted by a PIN. Do you believe this EMV would have averted those same targets?

Ms. ROCHE. It would not have averted the breach itself, but it would have made it very difficult to counterfeit the cards. It is difficult to counterfeit the chip in the card so the cards can then be used to commit fraud.

Mr. HARDY. This liability shift to the retailer or whatever you want to call it now instead of the banks, why the October 1st deadline? Does anybody want to care to address that? The busiest time of the year. We are going into the busiest approach of any retail market or any selling between now and December.

Ms. ROCHE. Yeah. The liability shift was announced August 2011, so more than four years ago, and typically around the time of other markets announcing their liability shift, October 1 has been a very commonly accepted date because we recognize that at that point in time we start to see increasing payment volume. So it was just a date to align with the same dates that many of the other parts of the world that announced their liability shift dates effective October 1. When we announced it in August 2011, we also made it October 1 of 2015.

Mr. HARDY. We, as in Visa?

Ms. ROCHE. We, as in Visa. Other payment systems had their own announcements of liability shift dates.

Mr. HARDY. So October 1 is only for Visa?

Ms. ROCHE. October 1 is for Visa. MasterCard also announced the same date later, but we announced that first in August 2011.

Mr. HARDY. Assuming that this all comes together over the next couple of years and we have 100 percent usage of EMV and the token and everything starts working but then the criminals always seem to find another, avenue. Is the liability shift still on the retailer or does it go back to the bank?

Ms. ROCHE. Well, so the liability shift actually, once the merchant has invested in chip technology, they are then protected from any liability for counterfeit fraud. And merchants are not having any liability for lost and stolen fraud, which is also commonly associated with PIN. So the liability shift is specific to EMV and counterfeit fraud. Once a merchant has made that investment in a chip terminal, they do not have liability for counterfeit fraud.

Mr. HARDY. Just to be very clear, once they have had that investment, then that liability goes back as it was?

Ms. ROCHE. Right.

Mr. HARDY. Thank you.

As EMV cards become more and more commonplace in the United States market liable for fraudulent card use if they have not upgraded the reader technology software, what will the cost of this upgrade cost for small businesses? Have you included all the other residual costs that they would have to implement? You know, training and the whole—has that cost been in the analysis? Because it seems awful low to me. I am a small business owner previously myself.

Ms. ROCHE. Many of the small business owners that we have been talking to in our 20 city tour, as well as working with the Chambers of Commerce and other parts of the industry, have mentioned that the upgrade to chip technology for some of them has been kind of like replacing a cell phone where they get a new device and they may change processors, they may shop around to get a better processing deal that actually may save them money compared to what they are paying today to process mag strip transactions. So for some of them, the upgrade to EMV chip technology is not only giving them that protection against counterfeit fraud liability, but many of them are futureproofing their business to accept mobile payments and investing in some other technology that may help them run their inventory or their supply chain and manage their businesses more effectively. So some of them are doing other investments and add-ons as they move to EMV technology.

But in terms of staff training, we have worked closely across the industry, not only on Visachip.com do we have a lot of training materials, including a 10-step implementation guide and downloadable sales associate training materials they can use, but we worked with MasterCard, American Express, and Discover to do a gochipcard.com site.

Mr. HARDY. I have another question I need to ask. I also want to know, in one of these comments here it sounded like there was not going to be that much liability at first, understanding it is a two to four year process. So how are we going to determine which business is going to reap that liability and which is not?

Ms. ROCHE. We have been doing a lot of education with the small business merchant community and the large retailers to identify which retailers tend to be the ones that have a high likelihood of counterfeit fraud. It is where you think it may be, like electronic stores, high-end luxury goods retailers, for example, whereas small businesses typically that are in the service industry or a local delicatessen, cafeteria, coffee shop, they are not typically the recipients of a lot of counterfeit fraud. So we have been doing education with the major retailers so that they know what their counterfeit fraud liability will be, as well as with the small business merchants and their supplying industry so that they understand what the counterfeit liability will be for them. We want the whole industry to move to this technology because it does help secure payments and preserves consumer confidence in payments, but at the same time, typical small business merchants that are doing services or low value transactions are not usually the recipients of counterfeit fraud.

Chairman CHABOT. Thank you. The gentleman's time has expired.

The gentleman from Hawaii, Mr. Takai, who is the ranking member of the Contracting and Workforce Subcommittee is recognized for five minutes.

Mr. TAKAI. Thank you. Thank you, Chairman, and thank you for having this hearing. I really appreciate this.

As someone who has had to change their credit card for each of the last three years, I think anything we can do to enhance protections and to prevent fraud is much appreciated. But I believe as any transition, it is very tough.

I have a few questions. I wanted to start with Ms. Roche regarding, well, here is my question. The merchant community has strongly advocated for this move to the chip and PIN system here in the U.S. In fact, I may add, I was going to Japan and a few other countries for quite a while. My Visa card had the chip technology for maybe three years now and I was not able to use it until just about two weeks ago here in the United States. In fact, in Hawaii. So as a credit union with many members going overseas, what has been your experience regarding the fraud rates on the PIN-enabled or the chip cards?

Ms. ROCHE. That is a difficult question to answer because the cards that we are issuing have the chip and a swipe on the back of it. So we had to. Because the cards are getting swiped in addition to being used as chips, we have had to reissue cards with chips that have had fraud committed on them. So our experience, it is very hard to segregate whether the fraud is coming from a chip-read card or a swiped card.

Mr. TAKAI. So the merchants are going to push us now to, if they have not been able to use the chip instead of the swipe, they are going to ask us to do it, although we could do both, either?

Ms. ROCHE. A lot of it depends on how the readers are programmed, but in my experience in using the cards, if there is a chip in the card and the merchant has the chip reader enabled, it will force you to use the chip side.

Mr. TAKAI. Okay. Okay. And do you know what is surprising? I have a debit card, too, and for the past year or so, some merchants do not require a PIN, so that was surprising. But on your credit cards, maybe your debit cards, you require a PIN. So are PIN numbers helpful? Do they prevent fraud? And then are they actually stored on the merchant's system?

Ms. ROCHE. So the PIN numbers are—what really matters, what is keeping the transaction secure is the chip. So the authentication method, whether it is PIN or signature, is not as important. And, in fact, the PIN is a static data element that can also be stolen. But what is most important is that the information on the chip is what is making it more secure because that is a random number, generated authentication method that changes every single time and cannot easily be counterfeited. That is what is most important about this transition.

Mr. TAKAI. Okay. Thanks.

And then to Ms. Ericksen, on your website it states that you are rolling out the Chip and Choice to give merchants greater flexibility on their payment options. Do Visa rules allow merchants to require PINs on every debit transaction if that is the flexibility they prefer?

Ms. ERICKSEN. We support PIN, as well as signature, as well as “no card holder” verification. So our rules provide flexibility for merchants and for issuers depending on the type of transaction that is being conducted. For example, transactions up to \$25 do not require a signature or a PIN, and transactions up to \$50 at grocery stores do not require a signature or a PIN either. So it gives the flexibility to the merchant depending on if they want to enable PIN or signature, or also be compliant with the rules and not require either signature or PIN for the transactions that qualify for that.

We do know that roughly 50 percent of the merchant locations in the U.S., particularly small business merchants, do not have the incremental security technology that would secure and encrypt that PIN, so many small business merchants have not opted to invest in PIN technology, but we do support that, whether or not on the issuing side or on the merchant side they want to invest in supporting PIN or signature.

Mr. TAKAI. Who has the liability for debit cards? I mean, the debit charge transaction goes directly into my checking account and pulls the money directly out. So do I have liability or do you have liability?

Ms. ERICKSEN. Consumers have zero liability for that. So from a Visa perspective, consumers have zero liability, whether it is a credit card transaction or a debit card transaction.

Mr. TAKAI. When was the shift done to eliminate the four PIN requirement for debit cards?

Ms. ERICKSEN. I do not understand your question.

Mr. TAKAI. Debit cards required the PIN for many years until, like I said, just about a year ago I was able to use my debit card without my PIN.

Ms. ERICKSEN. For many years you have been able to use your Visa debit card as a signature card or without a PIN for point of sale. Typically, if you are using it as a PIN, it is going over a different network that requires a PIN for that transaction, or to get cash back at the point of sale, or at the ATM, for example, but using it as a Visa card at the point of sale, you have always been able to use it without a PIN.

Mr. TAKAI. Really? Okay. Thank you.

I yield back.

Chairman CHABOT. Thank you very much. The gentleman's time has expired.

The gentleman from Missouri, Mr. Luetkemeyer, who is the vice chairman of this Full Committee is recognized for five minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman.

Just to kind of recap here, make sure I am understanding what is going on here, basically what you are trying to do, we have a problem. The problem is fraud and cyber theft that is occurring against financial institutions and through the system at which they are having a cost. Is that correct? They are trying to alleviate. So the solution to that is for the new chip and PIN, chip and whatever kind of technology. Is that correct? And the cost of this, if I get this correct, is borne by the banks or the transaction companies versus the merchants have a small cost to get a new terminal and some software, whatever, and then the consumer has zero cost. Is that all correct?

Ms. ERICKSEN. So the consumer has zero cost but it is shared across the industry in terms of the banks investing in reissuing the cards because chip cards are more expensive to reissue. And also on the merchant side in upgrading their infrastructure to be able to have the chip readers.

Mr. LUETKEMEYER. Did I hear a while ago that the cost to re-issue cards is 50 bucks?

Ms. ERICKSEN. To reissue a card is not. It is more the terminal side is roughly in the \$50 range. The card can be about \$1 to \$5 depending on the size of the institution and the number of cards.

Mr. LUETKEMEYER. Okay. What is the \$50 then?

Ms. ERICKSEN. The square reader is \$49 that a merchant can buy to accept payment.

Mr. LUETKEMEYER. Oh, okay. So that is a merchant cost.

Ms. ERICKSEN. It is a merchant cost.

Mr. LUETKEMEYER. Okay. So it costs then 50 bucks to be able to read the cards?

Ms. ERICKSEN. Right.

Mr. LUETKEMEYER. Okay. Okay, so knowing all that, are there complaints out there? What are the complaints about doing this? It appears that we need to do this. I know I can tell you from being in the financial institution business, you know, my institution, local institution got hit with some of these cyber deals and to me this is a concern from now on. Here in Congress, we have a responsibility to try and work to try and protect the government data, but also to help where we can the business and industry and consumers to be able to protect their data. And this is a huge problem. It is a burgeoning problem for our entire society and the world as a whole. And so this is something we are going to have to figure out over the long haul from now on because this is, you know, I think you used it a while ago, 70 percent of all transactions are with credit cards now. Is that correct?

Mr. TALBOTT. Electronic.

Mr. LUETKEMEYER. So if we are headed in that direction, we are going to have to be able to protect the data. That is a real problem. So I guess the concern is that we know what the problem is. You know it is going to be getting greater as the bad guys figure out how to get around the system. What are the complaints about doing what you are doing? What have you done to alleviate those, I guess?

Ms. ERICKSEN. Well, we have seen a lot of great momentum in the industry. And as I am sure Mr. Talbott can also elaborate on, but I think the key thing to remember is it is a shared cost and a shared effort across the industry. The issuers are reissuing the cards. The payment systems are investing in new technology to stay ahead of the criminals and to do more predictive analytics on the system side as well as those transactions are flowing through our networks. And the merchants are investing in the technology to be able to read chip as well as mobile as we are moving in that direction. So it is really a shared effort.

Mr. LUETKEMEYER. Okay. What is the amount of fraud reduction that you anticipate with EMV adoption?

Ms. ERICKSEN. Typically, in markets that move to chip technology, when they get to that 60 to 70 percent of their transaction volume in a country being chip on chip, it takes about two years after the liability shift date, we also see counterfeit fraud go down by about 60 or 70 percent and continue to go down as the penetration level goes up.

Mr. LUETKEMEYER. Okay. And a while ago you also talked about new technology. This enables you to do mobile technology on taking transactions on a mobile basis as well as you are looking at

biometric safeguards as well as encryption. At what point, or how quickly do you anticipate getting to that type of safeguard?

Ms. ERICKSEN. Tokenization is typically used on a mobile phone today or an ecommerce transaction. So tokenization today is where you put in your account number on your Apple Pay device, for example, and your account number is actually replaced with a different number, a digital token. So that is something that is becoming much more prevalent. It is already in use today in Apple Pay, for example.

Mr. LUETKEMEYER. Okay. So what about the biometric? How quickly is that?

Ms. ERICKSEN. Biometric is also being used in mobile technology as well. So when you do Touch ID to authenticate yourself to a smartphone, many more smartphones are enabling that. And so Touch ID and biometric is one way that is already being enabled, particularly on smartphones.

Mr. LUETKEMEYER. Okay. So we have it on a mobile transaction. What about a merchant? Is he going to be able to take that? How quickly do we move to that area?

Ms. ERICKSEN. We do not see that a lot in the face-to-face merchant environment using your card at a reader today because it is incremental investment in being able to do biometric. It is much more prevalent today on the mobile phones.

Mr. LUETKEMEYER. Okay. Well, how quickly do you anticipate that happening? I mean, I assume that, you know, I think there was a comment made a while ago about the PIN technology is not perfect. If the encryption is better, how long will it take to get there?

Ms. ERICKSEN. Encryption is a different technology. I do not know if you want to talk about encryption, Scott.

Mr. TALBOTT. Yeah. Sure. So encryption is being rolled out now. There are a number of companies that offer it to merchants if they would like to avail themselves of it. Some are and some have not. It is sort of behind this migration to chip, but it is out there and I suspect, Congressman, that it will move pretty quickly. Because what we will see, and this goes to your question, Mr. Chabot—

Mr. LUETKEMEYER. What kind of costs—if I can ask one more question real quick, what kind of costs are affiliated with it?

Mr. TALBOTT. For going to tokenization?

Mr. LUETKEMEYER. Yeah.

Mr. TALBOTT. It is marginal. I do not have those numbers exactly, but I know—

Mr. LUETKEMEYER. When you say “marginal,” is it 2 bucks, 20 bucks, \$200, \$2,000?

Mr. TALBOTT. It is a couple cents per transaction at this point.

Mr. LUETKEMEYER. Okay. All right. Thank you. I yield back.

Chairman CHABOT. Thank you. The gentleman’s time has expired.

The gentlelady from California, Ms. Hahn, is recognized for five minutes.

Ms. HAHN. Thank you, Mr. Chairman. I appreciate you holding this hearing.

So Ms. Ericksen, I understand what we are trying to do here. There was a problem. Visa and other banks are trying to incentivize merchants out there to switch to this new technology to reduce their fraud, so the big incentive was if you do not by October 1st upgrade your terminals to this chip technology, any fraud that happens, you, the merchant, are 100 percent liable for the fraud. Was that the—

Ms. ERICKSEN. There are some clarifications, too. In general, the direction is if a merchant does not invest in a chip terminal, they may become liable for any fraud if it is a chip card used at their store but the mag stripe is still read off of that card. So if it is a mag stripe card where the issuer has not invested yet in chip technology—

Ms. HAHN. Right.

Ms. ERICKSEN. If that mag stripe card experiences fraud at a merchant location that also does not have chip, it is still the issuing bank who is liable for that. So the merchant is only liable for any fraud at their location if it is a chip card that has been used at their store where they do not yet have a chip terminal and so they are reading the mag stripe on that card. If that turns out to be a copied mag stripe, a counterfeited mag stripe, then that merchant could be liable for that transaction. Yes. But it is not for mag stripe cards that have not yet been upgraded to chip, and once the merchant upgrades to chip, they are then protected from any liability?

Ms. HAHN. Correct. Okay. So it is a little confusing I think to some merchants, and in my district office in Los Angeles, we sort of did an informal survey of our small businesses, you know, about 30 of them. And it was surprising how many of them did not have any idea that as of October 1st they would be responsible for all liability under that scenario, the one you just described.

So I guess my question to you was I know you did sort of a 20 city road trip which did not seem like a lot of cities to me, you know, and there is a public website that people could go on but, you know, I know a lot of my small businesses, you know, kind of do not operate in that world of just automatically going on a website to see what is going on in their world. Do you really feel that you did a good job of communicating this? And just from my informal, unscientific survey, you know, a lot of my small businesses did not comprehend what was happening as of October 1st. Do you think you could do a better job? Or do you think maybe your communication failed to reach a lot of small businesses?

Ms. ERICKSEN. Well, as we said before, it does take about two or three years after the liability shift date to get to 60 to 70 percent adoption of chip technology, so we really are at the start line, and we have been doing a lot of education to this point, but we are also continuing. We are not stopping. So next week I am going to be in Chicago working with the Chamber of Commerce there, doing another small business education tour. Just last month we did the Small Business Development Centers Conference and educated the Small Business Development Centers who counsel and provide support for small businesses so that they would have the resources that they need to be able to provide that information. So we are

continuing to get the word out. We are not stopping. We are certainly trying to continue to get the word out.

Ms. HAHN. But just because you do not get the word out does not mean that that scenario that you described is not a reality.

Ms. ERICKSEN. Yeah. Well, their processors are also responsible for communicating that to them. So it is not only Visa and MasterCard in the industry but the processors that the merchants work with are getting that information out, and many of them are providing incentives for them to do an upgrade to this technology. And so there are many different touch points with the merchants to get the information out. Again, a lot of the counterfeit fraud is concentrated in more of the higher end retailers where you see high value transaction volume, not typically in a lot of the small business merchants.

Ms. HAHN. Right. Right.

Ms. ERICKSEN. But we are not going to stop in terms of our education efforts.

Ms. HAHN. Right. And you know, this is another issue, but I will say that my Visa card that is held by Wells Fargo sent me a letter with my—well, sent me the new chip card and then subsequent to that sent me a very serious letter saying that just to let you know, you know, this is—we are transitioning to the chip card. We can see that you are still using your other card. And I do not know how many people got that, but that freaked me out because I had already had one card compromised earlier, but I knew I had gotten rid of my other card. I shredded it, and so that upset me. When I went through the 1-800 number to call them, oh, that is a mass email we sent out to everyone. So I think that is unfortunate, and I talked to some other people who also with different cards had gotten that same mass email. And I think that is unfair to the consumer to send that sort of scare tactic letter saying they could see that I was still using my other card. And I do not know what we can do about that, but that is for another hearing.

Anyway, thank you. I yield back.

Chairman CHABOT. Thank you. And if it is of any consolation, when my wife and I got back from vacation about a month ago, we had a phone message indicating that the IRS was going to file a lawsuit against us the next week because we had not paid our taxes. And I said, “Did we not pay our taxes?” And we had, indeed, paid our taxes. So anyway, she went online and a whole lot of people were getting that same thing, so it is a scary world out there. But thank you very much.

The gentlelady from American Samoa, Ms. Radewagen, who is the chair of the Health and Technology Subcommittee is recognized for five minutes.

Ms. RADEWAGEN. Thank you, Mr. Chairman, and Ranking Member Velázquez. I also want to welcome the panel. Thank you for appearing today.

I have a couple of questions for Ms. Ericksen. I was hoping you could tell me more about Visa’s opt-in geolocation service called Visa Location Confirmation. I understand this service could benefit customers who travel, like my constituents back in American Samoa.

Ms. ERICKSEN. Yeah. Thank you, Congresswoman. Yes. Mobile Location Confirmation is a new service that consumers can opt into depending on their financial institution. More and more financial institutions are enabling this service, and it allows them to associate their mobile phone with their account so that we can detect whether or not their mobile phone and their purchase is happening within the same vicinity. So, for example, if your constituent is doing a purchase in New York but their mobile phone is in Los Angeles, we would score that transaction as higher risk and there may be a chance that that transaction would be declined versus if their transaction was occurring in Chicago and their mobile phone was also in Chicago, we would have better confidence that it is really then doing that transaction. So higher likelihood of an approval.

Ms. RADEWAGEN. Thank you.

As a member of a district that is comprised mostly of small businesses, I am concerned about the merchants in my district that can benefit from the EMV chip but cannot afford the transitional cost. Do you have any plans to offset this cost for such merchants?

Ms. ERICKSEN. Well, we know that based on the countries that have moved to chip technology in previous years, the incremental cost of moving to chip now in the U.S. is rather based in. So we know that roughly 30 to 40 percent of the terminals that already exist in the U.S. have the chip hardware slot in them but they may need a software upgrade. So in many cases they do not need a new terminal. They just may need a software download from their processor. And as we have mentioned, some of the costs that are available or the terminals that are available to merchants are now in the cost range of \$50 or \$49 for the square device and under \$100 merchants can buy a terminal at Costco for \$99, for example. And that device was even on sale for an additional 20 percent off last week. So we are seeing more and more low-cost and cost-effective solutions becoming available to the merchants.

Ms. RADEWAGEN. Wow. Thank you, Ms. Erickson.

Ms. ERICKSEN. Thank you.

Ms. RADEWAGEN. I yield back, Mr. Chairman.

Chairman CHABOT. Thank you. The gentlelady yields back.

The gentlelady from California, Ms. Chu, who is the ranking member of the Economic Growth, Tax, and Capital Access Subcommittee, is recognized for five minutes.

Ms. CHU. Thank you.

Ms. Erickson, as of July 1, 2015, the EMV Migration Forum estimated that only 25 percent of retailers would be in compliance with the October 1st deadline. Previous estimates had been as high as 44 percent of merchants meeting the date. Are we behind in terms of the adoption? First, I would like to know the answer to that.

Ms. ERICKSEN. Yeah. I think there have been different estimates depending on if it is coming from AITE Group or the Payments Security Task Force or EMV Migration Forum that have all been roughly projecting that by the end of this calendar year, roughly 40 percent of the terminals would be upgraded by the end of December of this calendar year. And so as we were mentioning before, we know it takes several years to get to critical mass of adoption, and we have seen quite a bit of significant momentum

with the 314,000 locations as of September 15th, and even more locations that came on just in the last week and are planning to come on this month. So I would say there has been great participation in the merchant community in terminalizing and updating those terminals to be able to accept chip cards. And even more plans for that to continue to roll forward in 2016 and 2017, which is very similar to what we have seen in other countries that have moved to chip.

Ms. CHU. Have you done a poll as to what the main issue is in terms of adoption? Is it ignorance or is it the expense?

Ms. ERICKSEN. I think it is mainly just planning that into their implementation time. Many large retailers have just recently announced that they have enabled nationwide whereas they were previously piloting in 50 to 100 stores to fine tune the solution, train their sales staff, make sure that they had the solution operating the way that they wanted it to operate before they rolled it out nationwide; whereas, some small business merchants have been upgrading as their processors have been providing them the solution. So it depends if you are a major retailer or a small business owner as to how that migration is going forward. But we have actually seen quite a few major retailers enable in just the last week or two and more even planning to go forward.

It is also important to note that roughly 50 percent of the volume we see today has been coming from small business merchants, so many members of the small business community have been upgrading to EMV and are continuing to do so as they go forward.

Ms. CHU. So in these other countries that you mention, such as Brazil and Canada and, of course, EU, are they at 100 percent compliance now?

Ms. ERICKSEN. They are at roughly 90 percent, so it did take about four to five years after the liability shift date in each of those countries to get to 90 percent. There are still some cards and some terminals, in Australia and Brazil, for example, that are not 100 percent updated to chip. So it really depends. There are still some merchants that may decide that they are going to wait, and there are still some issuers that have not reissued all of their cards. But that is really the benefit of the liability shift, is it provides that incentive but it is still ultimately the end party's final business decision as to whether or not they invest.

Ms. CHU. And have they been able to successfully reduce the fraud in those countries?

Ms. ERICKSEN. Yes. We have seen typically around the time of the liability shift date, two years after that they got to 60 or 70 percent of their volume being chip on chip. The criminals tend to do a last run at counterfeit fraud right up to the liability shift and a couple months and years after until they get to 60, 70 percent of their volume being chip on chip, and that is also when we see that counterfeit fraud start to go down is when a country gets to around 60 percent of their volume being a chip card used at a chip terminal.

Ms. CHU. And Mr. Weston and Ms. Roche, you talked about supporting H.R. 2205, the Bipartisan Data Security Act, which would apply Gramm-Leach-Bliley standards for all industries that handle sensitive financial institutions. Can you elaborate on the data secu-

rity measures that you have to meet under this act? How would this change for all of the other merchants that you think should have these kind of standards?

Mr. WESTON. I think the important thing here is that any entity that is handling consumer financial information needs to have some respect for the privacy of that information and the duty to protect it. Today there is not a clear national standard, a federal standard, that everyone who handles that sort of information has to abide by. Financial institutions, be they credit unions or banks, are certainly subject and are regulated and examined. The retail industry today has no standards.

Ms. ROCHE. And I will add that the details are provided in my written testimony, but agreed. The national standards would be very important to ensuring that the data is not breached, it is not taken.

Ms. CHU. Okay. Thank you. I yield back.

Chairman CHABOT. Thank you. The gentlelady yields back.

The gentleman from Illinois, Mr. Bost, is recognized for five minutes.

Mr. BOST. Thank you, Mr. Chairman. And I guess my first question is to Mr. Talbott. When you show the swipe device and you say it is about \$50, and there are many makers of that device, are they already competing them on a price basis for the merchants? I know every place we go, it does not matter whether it is to take a cab, barber shop, wherever, that they are using—if they do not have, if they are not a larger merchant, whether it is in their cash register or they are available right there at the register, they have those. So do you see a competition on those?

Mr. TALBOTT. Yes, sir. The payments industry is highly competitive, and there are a number of players who can provide a card reader, whether it is an actual equipment device maker, processors can cut a deal. Everyone is trying to get the merchant's business, and they are competitive both on the price of equipment as well as services.

Mr. BOST. So with that, are we seeing the education? Because as a small business owner myself, I know that there are many that do not know and do not understand the liability that is going to be put on them. Do you think that those companies then are also trying to educate and let people know? And then how many times, as a small business person, do you realize when somebody sends you something you think, "Oh, yeah, that is just make-believe. I am not going to respond to that."

Mr. TALBOTT. I think everyone in the industry, at least ETA members, are actively pursuing education as well as financial incentives to offer to small businesses to let them know this is a perfect opportunity. If you service a small business, your processor could reach out and talk to them, talk about an equipment upgrade, talk about the change, talk about what the liability shift means. There is also a lot of negative noise out there that we are working to fight through. Critics are arguing that this is not great, which is inaccurate in the sense of the ability of chip to reduce fraud, counterfeit card fraud. But the efforts are being made both education-wise in all forms, as well as financial incentives are being offered.

Mr. BOST. Have you heard of any, I mean, everybody thought it was safe when you first had the swipe. You know? I mean, when cards first came out we thought they were safe. Criminals are always going to be looking for something else to put on there.

Mr. TALBOTT. That is right.

Mr. BOST. And do we see already somebody trying to offset this?

Mr. TALBOTT. Well, I think that there is always going to be—we will build a 10-foot wall and crooks will build an 11-foot ladder, and so we must be continuously vigilant, as well as pulling multiple layers of protection, whether it is EMV, tokenization, encryption, or biometrics, we need to keep moving the system forward because the crooks will continue to fight to try and go after the money. So devaluing the information is the first step, and that is what tokenization, as well as chip does.

Mr. BOST. Just another question if I can, because I have the panel in front of me and I wanted to find this out. The responsibility of the merchant to ask, or their agent to ask for an ID along with the presentation of the card, is that still pushed for?

Mr. TALBOTT. Not at this point. It is a fallback, but it is not necessarily common practice.

Mr. BOST. Okay. Because my wife, I mean, she always thanks people if they do that, and I have watched her do that. And so many people, we just do not think about it.

Ms. ERICKSEN. Yeah. No, merchant does not have liability for lost and stolen fraud, so typically checking an ID and all of that would be associated with that. So the merchant is actually protected against any liability for lost and stolen fraud. There are some merchants that may want to ask for an ID, particularly some gas station merchants sometimes do that where they will ask for an ID and we do allow that, but we do not require it.

Mr. BOST. Okay. All right. Thank you, Mr. Chairman. I yield back.

Chairman CHABOT. Thank you. The gentleman yields back.

The gentlelady from Michigan, Ms. Lawrence, is recognized for five minutes.

Ms. LAWRENCE. Thank you, Chairman.

I am very sensitive to the larger financial institutions and the smaller financial institutions. So my question today will be directed to Mr. Weston and Ms. Roche. You represent the small and mid-size financial institutions. I would like to understand from your perspective, we talked a lot about liability for the merchants and for the industry, but let us drill down to your piece of the market. What types of costs do you incur? What is the impact on you as a smaller financial in notifying your customers or responses to breaches? So would you please elaborate on that?

Ms. ROCHE. So at our credit union, we take breaches very seriously because we know how disruptive they are to the consumers. I think someone on the Committee mentioned how difficult it is when your card gets compromised to get the new card, activate it, get all of your authorized payments set up again, so it is very difficult and concerning problem. It does not feel good. You have been compromised. So what we do is proactively make phone calls when there is a breach, such as a large Target breach or Home Depot where so many cards have been compromised. We get a list. Typi-

cally, we get a list of those cards that might have been involved in that, and we reach out to the consumers, our members, on an individual basis to let them know that their card may have been compromised, and then we give them the option, the choice of whether or not they want the card reissued. And that is probably a much more pro-consumer way of handling it because otherwise, you are forcing the consumer to switch the card out and—

Ms. LAWRENCE. And Ms. Roche, if I could just say, you know, there is a difference between your local credit union and the national financial institutions. One of the things I hear a lot is that personal touch. But what I wanted to drill down, what is the impact financially, because you do do that personal outreach? Is it going to be a greater impact on you with the chip or less of an impact? So that is where I am trying to go.

Ms. ROCHE. So that is a great question because really, the EMV in the chip is a first step and only helps with one type of fraud that is being committed. And then we have also talked about all these other different technologies that are coming in to play to help combat the other ones. But what NAFCU and our credit union supports is that there is H.R. 2205, to implement a national data security standard, because that is going to keep everyone looking forward. It is going to put some of the same requirements on all businesses, that financial institutions are already having to comply with, and it will make the consumer information much more safe and secure.

Ms. LAWRENCE. Thank you.

Mr. WESTON. I would just add that I think doing something to combat the breaches, whether it is convincing the organizations, be they healthcare providers or retailers to step up to data security standards that are the equivalent of what the financial services industry does, the chip card deployment, certainly, anything we can do to make the information better protected, to make it much more difficult for the bad actors to utilize it if it is available to them, that is going to be helpful to the community financial institution as well as to the consumers because they are not going to have the disruption in their lives of being on a trip and having their card be shut down and having to get another one overnighted, et cetera. It is an expense for us but similar to what Ms. Roche indicated, we look at it as a high-touch service. We have got to be there for our customers. That is the community bank way of competing. And so it is a necessary expense.

Ms. LAWRENCE. I just wanted to follow back on what Ms. Erickson said. I am refreshed that, or encouraged that you are going to continue the education, that you will continue to do the briefings. It is good to know that the providers are also doing some outreach to the small businesses. Because one of the challenges, as you know, to small businesses is the asset to information and education. And so I really, any way that we can enhance that with public announcements or anything that we can do through our chambers, I really encourage that.

Ms. ERICKSEN. Thank you.

Ms. LAWRENCE. Thank you.

Chairman CHABOT. Thank you very much. The gentlelady's time has expired.

Ms. LAWRENCE. I yield back.

Chairman CHABOT. Thank you.

The gentleman from South Carolina, who is the chairman of the Subcommittee on Economic Growth, Tax, and Capital Access, is recognized for five minutes.

Mr. RICE. Thank you, everybody for being here. I find this really interesting. It brings me back to my commercial paper classes in law school. And the shifting of liability is certainly a worrisome but understandable thing. It sounds like everybody on the panel thinks this is a good idea. I have not heard anybody argue against it.

The chip cards only help for in-person transactions; right? So what percentage are in-person versus others? Can anybody quote those statistics?

Mr. TALBOTT. I think of the total fraud, Congressman, about half is instore, and of that, about two-thirds is in-person. So we are talking about 3.5 or so billion a year.

Mr. RICE. Half and two-thirds?

Mr. TALBOTT. Half of all fraud is online; half is instore. And of that half that is instore, two-thirds is counterfeit fraud. Counterfeit fraud.

Mr. RICE. Okay. And you say that encryption is the biggest tool you have to fight online fraud; right?

Mr. TALBOTT. Yes, sir.

Mr. RICE. I mean, for years I would not put my credit card on the Internet, and I finally broke down and now it is a routine thing and it is amazing that it does not happen more than it does.

Does this proposed—this regulation commit small businesses to any future upgrades or just this one instance?

Ms. ERICKSEN. The liability shift is just for an upgrade to EMV.

Mr. RICE. That is it?

Ms. ERICKSEN. That is it.

Mr. RICE. And so when you come up with your next best thing, they are not committed to do that?

Ms. ERICKSEN. We are encouraging that when they are making that infrastructure upgrade for EMV to protect against counterfeit liability, that they also consider contact with an NFC which enables them for mobile phone acceptance because it is a very similar upgrade and many times the equipment does both. So to make sure—

Mr. RICE. What I am worried about is you are going to come up with something greater two years from now that they are going to be required to do that or there will be a liability shift. There is nothing in there that requires that.

Ms. ERICKSEN. In other countries around the world, when they have moved to the EMV liability shift, that has been the key driver.

Mr. RICE. Let me ask you this. Earlier people were talking about the difference in liability for debit versus credit cards, and you are saying the consumer has no liability for either. I have always heard debit there is a little bit more concern there, but what about Internet banking transactions? You know, I log onto my bank and I put in my account name and my password and I can move

money. Who is liable for that? If somebody stole my password and my account name, who is liable for that?

Ms. ERICKSEN. I will leave that to my banking—

Mr. WESTON. I believe the rules would apply that it is between you and the bank that you have chosen for your PC banking service. So as a customer of that financial institution, you need to look to their policies as to—

Mr. RICE. So there is no law. Like, the old law that the bank is supposed to know your signature on your check and that is your problem if it has been forged.

Mr. WESTON. Certainly, if you are transferring money in and out of your account, there are rules that apply to electronic funds transfers. Yes.

Mr. RICE. All right. One thing that has bothered me in the past as a user of credit cards is when—it has not happened very often, but I might be in a store to buy something and my credit card gets declined, and I go outside and I call the credit card company and they say, you know, this actually happened to me. They said, “Well, at 3 o’clock in the morning your card was used to sign up for Vonage. We do not think that was you.” Well, they were right. It was not me. \$14.00. They were right. Should they not have some duty to notify me about that before I am standing in a—

Ms. ERICKSEN. So many issuers do have the ability to give you an alert. So this happened to me not that long ago. I was—

Mr. RICE. I hear “ability,” but should they not be required to notify me before they start declining my card on in-person transactions because some guy in Russia is doing Internet transactions for \$14 to Vonage?

Mr. TALBOTT. I think the challenge of that type of law might be overinclusive and inconclusive at the same time. There are so many different variations of that pattern, and we all have experienced it, that the industry is actually ahead of that and they will notify customers. I get notified frequently, so the industry has taken that step. I think a law would be difficult to implement.

Mr. RICE. How difficult is it for somebody—let us say I go into a restaurant and a waitress writes down my credit card number and expiration date and name. How difficult is it for somebody with that information to create a dummy credit card and use it in person?

Mr. TALBOTT. It is actually very simple. The technology for your mag strike is about 40 years old. It is the same technology used in cassette tapes, if you remember those. So it is easy for them to take the information and create a counterfeit card. And that is really where chip comes in, is that waitress would not be able to use that fake counterfeit card in stores. She could use it online, and that is where tokenization comes in, but it is actually very simple, which is why this step is necessary to end that counterfeit card fraud.

Mr. RICE. My time is up. Thank you very much. It has been certainly educational.

Chairman CHABOT. Thank you. The gentleman’s time has expired.

The gentleman from New Jersey, Mr. Payne, is recognized for five minutes.

Mr. PAYNE. Thank you, Mr. Chairman, and to our ranking member. And the gentleman from South Carolina, I tend to agree with you. This has been very educational. For some reason I have more problems with the cards I use than I have ever wanted to imagine.

Mr. RICE. Mr. Payne, it seems like I agree with you a lot.

Mr. PAYNE. Absolutely. Let me just ask, and this is for Ms. Ericksen or Mr. Weston. I am concerned about that the EMV required will affect small banks. In my district I have the only African-American owned bank in the State of New Jersey and, you know, naturally, it is a small business. Minority banks control about \$5 billion in assets as compared to say a Wells Fargo, that by itself has some \$1.7 trillion in assets. It is estimated that it costs banks and credit unions approximately \$3.04 for non-EMV cards, but the cost to produce the new EMV cards is almost twice that cost at approximately \$5.81. How can we ensure that small business banks and credit unions are not put at risk because of these requirements?

Mr. WESTON. Well, speaking from the community banker standpoint, I think the best way for smaller issuers to participate is through a combined program where we combine the buying power of those banks and collectively do processing arrangements or purchasing arrangements to bring those costs down to what is a more competitive figure to help them out. That is certainly what we have been doing at ICBA.

Mr. PAYNE. Okay.

Ms. ERICKSEN. Yeah. And from a Visa perspective, we are certainly working across the industry to drive down the cost as much as possible by streamlining the implementation process, streamlining the certification process, so when those banks come online to enable their backend system to process that chip one-time code through the system, we have done a lot to drive down that cost of implementation certification and enabling that chip technology to go through the system.

Mr. PAYNE. Okay. Thank you.

Ms. Roche, you know, your testimony, you stated that in the United Kingdom, online fraud rose 79 percent after their EMV transition. Online fraud in the UK has doubled as well. Based on these facts, we can presume that the U.S. should soon expect a significant spike in online fraud. And with the holiday online shopping season quickly approaching, this is a major concern. In your testimony you mentioned tokenization and cardholder verification technologies as an answer to online fraud. When should we expect this transition, and how will it work, and how will the liability shift work?

Ms. ROCHE. So I may yield to one of the other experts at the end of the table about when they expect those technologies to come into play, but what we think about at our credit union is that there is always going to be something else coming down the pike. And so the best way to protect the consumer data and protect the payment system and keep that fully functioning is to have a national security—data security standards in place. And that is where the H.R. 2205 becomes important because it gets all of us focused on

making sure that we are staying ahead and keeping up with the latest technologies and play and keeping the information secure.

Ms. ERICKSEN. As it relates to the other technologies, we really look at them as a layered security approach in working together. So from a chip perspective, as we mentioned earlier, there is already more chip cards in the U.S. from an issuance perspective than any other country. And on the merchant side we are seeing more and more merchants enable chip acceptance every day. End-to-end encryption also protects that data when it is in a merchant's system. It makes it harder for a criminal to break in and get that data, but when we move to more and more of the transactions being chip transactions, if a criminal breaks in and gets that data, there is a lot less they can do with it. They cannot use it for counterfeit fraud, for example. So encryption and chip technology work together. Encryption secures the data from being accessible and EMV chip data makes that data less valuable to a criminal if they get it. And then tokenization works well also for the online environment and for mobile applications where we are replacing the account number with a different number, so that way if the criminal gets that, they also cannot use it for anything. They cannot use it for counterfeit card fraud and they also cannot use it for online fraud either.

Mr. PAYNE. Thank you. I yield back.

Chairman CHABOT. Thank you. The gentleman's time is expired.

I will now recognize the ranking member for a statement or question.

Ms. VELÁZQUEZ. A last question. Do you expect financial firms to phase out magnetic strips in the future?

Mr. TALBOTT. We are going to have to run two parallel systems for a while, but eventually magnetic stripe will drop to very small percentages.

Ms. VELÁZQUEZ. Okay. All right. Thank you.

Chairman CHABOT. I have a quick question and then just a final point. I think it was you, Mr. Talbott, that talked about when we build the 10-foot wall the bad guys were up an 11-foot ladder. I assume that you all are thinking of those things relative to this, and if so, would you want to comment on that without telling the bad guys what you are up to?

Mr. TALBOTT. Sure. Here is the secret passcode.

As we develop these technologies to deal with threats, we are also looking to develop, and we are developing other technologies, whether it is geolocational, whether it is biometrics, whether it is facial or voice recognition. All of those are in the works. Thumbprints are already in play in a number of mobile phone applications. So we are constantly working and committing resources on R&D to develop new types of technology, dynamic types of technology to address future frauds and to make the system more secure. So we are constantly vigilant.

Chairman CHABOT. Thank you very much.

Ms. ERICKSEN. We are continuing to invest also in other technologies that use the analytics in the system. For example, we just announced a few months ago something called Visa Transaction Advisor, where we send a code actually to the gas station, to the

gas pump, that detects whether or not that might be fraudulent that would prompt the cardholder to then go into the store where the gas station attendant could maybe ask for ID to make sure it is really the real person. So we are investing not only in point-of-sale technology that helps detect fraud and possibly ask for a higher level of authentication like an ID, but continuing to invest in those predictive analytics that detect fraud patterns as well. So the technology is continuing to advance. There is also some work in the industry called 3D Secure 2.0 which is going to allow the sharing of data, like IP address and billing and shipping address matching for Internet or online transactions that will help better predict any fraud in the online environment. And so there are continuing advancement that are happening there as well.

Chairman CHABOT. Thank you.

And I think we heard from a number on both sides of the aisle, members who indicated that this was very helpful, and I think we learned a lot. Hopefully, the public did as well in educating people about what is happening here. And as I mentioned in my opening statement, it is the Committee's intention to have another hearing in a couple of weeks to allow all the merchants and small business folks and retailers to come in and voice their concerns to the Committee so we can delve into this further and make sure we are getting a complete picture of what is happening out there.

And I want to thank our witnesses for participating today. I would ask unanimous consent that members have five legislative days to submit statements and supporting materials for the record. And if there is no further business to come before the Committee, we are adjourned. Thank you.

[Whereupon, at 12:40 p.m., the Committee was adjourned.]

A P P E N D I X

Statement of

Stephanie Ericksen

Vice President, Risk Products

Visa Inc.

House Committee

on

Small Business

Hearing on

Transition to EMV Chip

October 7, 2015

Chairman Chabot, Ranking Member Velazquez and Members of the Committee, my name is Stephanie Ericksen and I am Vice President of Risk Products at Visa Inc. Thank you for the invitation to appear before the House Committee on Small Business to discuss Visa's ongoing efforts to help transition the US to EMV chip technology and what this means for small businesses.

For more than 50 years, Visa has enabled people, businesses and governments to make and receive payments across the globe. As a global payments technology company, we connect financial institutions, merchants and governments around the world with credit, debit and prepaid products. Visa works behind the scenes to enable tens of millions of daily transactions, powered by our core processing network—VisaNet. We make digital commerce more convenient, reliable and secure. It's important to note that Visa does not issue credit or debit cards or set the rates and fees on those products—our financial partners do.

Data breaches in recent years have highlighted that no business or industry is exempt from cyber threats, and, everyone—from consumers and small businesses to corporations and governments—are the targets. In today's connected world, it is critical that all those in the payments systems—payment networks, merchants, and financial institutions—work together to protect sensitive information and continue to drive advancements in security. At Visa, nothing is more important than maintaining trust in the payment system and we continue to place security at the forefront of everything we do.

Given the current cyber threats, especially those that merchants face, we need to move the payments industry away from static account information that can be stolen and used for fraud, to smarter technologies that make stolen account information useless to criminals. Chip is an important part of this fundamental change in the payments system, and we're committed to helping consumers and businesses make the shift.

EMV Chip Technology

This morning, I look forward to sharing with the Committee Visa's efforts to encourage the adoption of EMV chip technology in the U.S., as well as our work to educate and empower small businesses during this important transition period. For those who are unfamiliar with chip cards, or smart cards as they are often called, let me provide an overview of what they are, how they work and how we got to where we are today.

An EMV chip is a microprocessor that is embedded in a payment card or in other form factors such as a mobile phone. When a consumer uses a chip card at a chip terminal, a unique, one-time-use code, or 'cryptogram' is generated for each transactions. This type of authentication, which introduces dynamic values for each transaction, adds a substantial layer of safety. Chip cards effectively prevent counterfeit fraud, virtually eliminating one of the common ways criminals use stolen payment data. Since chip technology makes it essentially impossible to counterfeit cards, which is ap-

proximately two-thirds of the fraud that occurs in stores today, merchants will be less attractive targets for criminals.

Chip technology is also the basis for future payments innovation because it enables technologies like near field communications (NFC) technology and tokenization. When small business owners upgrade to chip-enabled terminals, they aren't just investing in payment and data security. They are also positioning themselves to accept the next generation of secure payment technologies, such as mobile and digital payments.

The payments system in the US is larger and more complex than any other in the world, with thousands of financial institutions and millions of businesses accepting electronic payments. In August 2011, Visa announced a roadmap to transition the US to chip technology through a set of milestones intended to encourage both issuers and merchants to adopt the chip technology. Visa's EMV chip roadmap is not a mandate. Instead, it provides marketplace incentives to encourage adoption by financial institutions and merchants—elements that have proven to be effective in moving other markets to deploy chip technology and thereby drastically reduce counterfeit fraud.

As part of the incentive program, Visa rules specify that, as of October 1, 2015, liability protection from counterfeit fraud on in-store payments is extended to the party that makes the investment in chip technology. The party that has not implemented chip technology, be it a bank that chooses not to issue a chip card or merchant that cannot accept a chip card, may bear the loss from any resulting counterfeit fraud. This shift applies to in-store, point-of-sale environments. Due to the complexities and life cycles of Automated Fuel Dispensers (AFDs) and ATMs, their liability shift will take effect October 1, 2017.

Education of Small Businesses a Top Priority

Throughout the ongoing transition to chip, Visa has dedicated significant resources to raising awareness and providing small businesses with the tools and information they need to adopt chip technology. In March, Visa launched our 20-City Small Business Chip Education Road Show to help business owners understand the value of chip card technology and to increase chip card acceptance. To date, we've traveled to 16 cities including Cincinnati, Charlotte, San Francisco, Boston, Houston, Miami, New York, Albuquerque, and Denver—to name a few. More than 1,000 small businesses owners have turned out to learn about chip technology from experts in payment security. To amplify our efforts, we are working closely with other partners, organizations and clients that provide critical resources to small businesses, including the Small Business Administration, America's Small Business Development centers, Facebook, the National Federation of Independent Business, and local chambers of commerce across the country.

Our efforts to educate small business owners does not stop there. On top of our dedicated chip education website—www.visachip.com—which contains specific information for all of our stakeholders, we also created an online toolkit specifically for

the small business community (www.visachip.com/businessstoolkit). With easy-to-use navigation, small business owners can quickly access actionable information about chip technology including a step-by-step guide to adopting chip, videos, and infographics at their convenience.

A key success factor in the transition to chip technology is ensuring a seamless checkout experience. To address this, our toolkit provides employers with a training module to ensure their employees know and understand how to use chip technology; it includes decals to place at the point-of-sale alerting customers that they accept chip cards, as well as instructions on how to complete a transaction with a chip card. Visa is making all of these materials available free of charge to merchants.

We have also focused on addressing the most significant barrier to adoption small business owners face: cost. Visa has worked with the terminal providers to make transitioning to chip technology more easily accessible, especially to smaller merchants. Low-cost chip terminal options are available for less than \$100 and, in many cases, the terminal is included in the cost of the service. For example, Square, a leading merchant processing services provider, recently announced a new \$49 card reader that accepts EMV chip cards and Apple Pay. Square is giving away 250,000 of them for free to small business customers and will also take on the risk of counterfeit fraud after October 1 if the merchant pre-ordered a device.

And, this is just one example. Other terminal providers like Chase, Bank of America Merchant Services, and VeriFone, to name a few have several low-cost options available to small business owners that bring that help prepare them for the future of accepting all payment forms including chip cards and mobile payments.

We know that our efforts to educate and facilitate the small business community are gaining traction. In fact, in August 2015, nearly 50 percent of the nearly 4 billion dollars in Visa chip transaction volume occurred at small businesses.

Chip Adoption Gaining Momentum

While we want to encourage a speedy migration to chip technology to improve the security of payments everywhere, we know that some businesses may take more time to upgrade. Owners of small businesses that do not experience significant loss from counterfeit fraud, such as dry cleaners, restaurants, or hair salons, may decide to upgrade to chip as part of their normal terminal replacement cycle. The roadmap was designed with this type of flexibility in mind, allowing businesses to make the transition on a timetable that meets their needs. Some merchants, for example, were ready this summer ahead of the liability shift, while others in the coming months.

In other words, October 1 marked the beginning of a process that will ultimately lead to near-universal adoption of chip technology in the US. With the milestones achieved to date, the US is well-positioned to adopt the next level of payment security for consumers, businesses, and financial institutions.

Where are we today?

Over the past twelve months we have seen significant progress. Today, there are more than 150 million Visa chip cards in circulation in the US, an increase of over 655 percent in the last year alone. That number eclipses the roughly 129 million Visa chip cards in Brazil and 124 million Visa chip cards in the United Kingdom, making the US the largest chip market in the world.

Retailers, and particularly small businesses, are making great strides in implementing chip technology. As of September 15, chip-enabled devices are in use at more than 314,000 merchant locations, representing a 470 percent year-over-year increase. We are strongly encouraged by the number of small businesses that are already using this technology and look forward to continuing to encourage their adoption of chip.

Tokenization

While EMV technology eliminates in-store counterfeit card fraud, it does not prevent all types of fraud—particularly fraud that occurs online in the e-commerce environment. To mitigate the growing risk of e-commerce fraud, Visa developed tokenization.

Tokenization, which removes the account number from the payment process completely, is one of the most promising technologies for fighting fraud. Tokenization replaces the account number's 16-digit account number in a payment transaction with a unique digital “token” or proxy number that is tied to the underlying account. Tokenization can enhance transaction efficiency, improve cardholder privacy and data security, and may enable new types or methods of payment. When fully deployed, tokenization in combination with chip, could virtually eliminate the need for merchants, digital wallet operators or others to use cardholder account numbers.

Cardholder Verification Technologies

Mobile payment applications such as Apple Pay, Android Pay, and Samsung Pay each offer enhanced security to consumers and merchants by using tokenization solutions to prevent the underlying card number from being comprised. And, as some of you may know from personal experience, many of the new mobile payment devices and applications use biometrics to verify your identity—like a thumbprint—before you can complete a transaction. At Visa, we believe this type of dynamic authentication is the future.

Today, with expertise gained from years working with merchants and issuing banks, Visa supports a variety of cardholder verification methods, including signature, PIN, and no cardholder verification for low value, low risk transactions. However, we see dynamic, or one-time use, verification technologies as the way forward. Just as the information technology industry is looking to replace the static password with more dynamic technologies, the payments industry must also replace static technologies in the payments ecosystem with more effective protections. I want to share

a few of these future technologies with you, some of which are exist today.

In February, Visa launched a new opt-in service that uses mobile geo-location information to more reliably predict whether it is the account holder or an unauthorized user making a payment with a Visa account. By matching the location of the cardholder through a cell phone or other mobile device to the location of the purchase, this service helps improve fraud detection and identify unauthorized transactions.

In addition, Visa introduced a new specification just last month to use biometrics with chip and transactions. The specification can enable fingerprint, palm, voice, iris, or facial biometrics in the authorization of payments. This first-of-its-kind technology framework is designed to work with the EMV chip industry standard to help ensure open, globally interoperable solutions for payment security. This product addresses increasing demand for biometrics as a more convenient and secure alternative to signatures or PINs, especially as biometrics technologies become more reliable and available. The architecture Visa has designed enables fingerprints to be securely accepted by a biometric reader, encrypted, and then validated. The specification supports “match-on-card” authentication where the biometric is validated by the EMV chip card and never exposed or stored in any central databases. Issuers can optionally validate the biometric data within their secure systems for transactions occurring in their own environments, such as their own ATMs. This innovative technology is just rolling out, but has great promise for protecting consumers in years to come.

Conclusion

We have come a long way in the past year as the US transitions to EMV chip technology, but, we must continue to work together to achieve the necessary progress to protect all stakeholders in the payments space, including small businesses. Visa is committed to continuing our work to drive innovation and ensure that EMV chip technology, tokenization, geo-location, biometric authentication, and other technologies evolve to address the needs and threats of tomorrow. This is critical for the success of our merchant and financial institution clients, and we look forward to working with all stakeholders on this important goal.

Thank you again for the opportunity to testify today. I would be happy to answer any questions you may have.

**Testimony of Scott Talbott,
Sr. V.P. for Government Relations,
Electronic Transactions Association (ETA)**

House Small Business Committee

Hearing on the

EMV Deadline and What It Means for Small Business

Oct. 7, 2015

Introduction:

Chairman Chabot, Ranking Member Velazquez, and members of the Committee. I am Scott Talbott, Senior Vice President for Government Relations of the Electronic Transactions Association (ETA). Thank you for inviting ETA to testify on the EMV transition and what it means for small business.

By way of background, ETA is a global trade association whose mission is to advance the payments technology. As the trade association of the payments industry, the ETA represents more than 500 of the world's most innovative payments and technology companies, from Fortune 500 financial institutions, to small, local sales organizations, to the world's largest technology companies. ETA's members are dedicated to providing merchants and consumers in our country the safest, most reliable, most secure payments system to facilitate commerce and power our economy—and the EMV migration is another major step forward in this regard.

The Electronic Payments Ecosystem—Driver of Economic Growth:

To help put the electronic payments industry into context, when consumers buy something from a merchant, they often will use a form of electronic payment, such as a credit card, debit card, gift card, prepaid card. Purchases can be made in person with the card or with a mobile device, or remotely, over the phone or the Internet. While the transaction is simply and securely completed within seconds of a swipe, dip, or tap, it involves an enormous and complex electronic payments ecosystem, which includes:

- consumer card issuing banks;
- the card brand networks that connect merchants and consumers;
- payment processors that connect merchants with networks of banks (issuing and acquiring) to ensure the transaction is authorized and processed;

- point of sale equipment hardware and software companies;
- program managers that work with consumers and issuing banks to help consumers obtain credit and prepaid cards;
- enablers of payment technology and e-commerce;
- merchant acquirers, which provide payment acceptance services;
- independent sales organizations that work directly with merchants to provide access to the payments system;
- sponsor banks, which establish policies for merchant acquirers, sponsor their registration with the card brands, and hold the risk of payment;
- anti-fraud companies that work with providers in the ecosystem to help ensure fraudulent transactions do not occur; and
- security companies that work with all other providers in the ecosystem to protect and secure transactions against intrusion.

This ecosystem is largely invisible to consumers and merchants because it works seamlessly to process billions of transactions each year—that’s literally thousands of transactions every second. Electronic payments are key drivers of commerce and economic growth in our country. To put this into greater context: 70% of U.S. GDP is attributed to consumer spending, and 70% of consumer spending is done electronically. Last year, electronic payments surpassed \$5 trillion and electronic consumer spending will only continue to grow. Indeed, my 2017, we project that ETA member companies will process \$7.3 trillion in consumer spending in the U.S.

The Electronic Payments Industry’s Commitment to Securing Customer’s Information:

ETA member companies take seriously their affirmative and continuing obligation to protect the confidentiality and security of their customers’ information. Our payments systems are built to detect and prevent fraud—and to insulate consumers from any liability. In fact, consumers in the United States choose electronic payments over cash and checks in large part because they have zero liability for fraud, making electronic payments the safest and most reliable way to pay. The liability is borne by companies in the payments industry due to Federal law and even more stringent payment network rules. In light of this financial responsibility and a desire to preserve consumer confidence in the security of electronic transactions, ETA members have a strong interest in making sure fraud does not occur, including through the misuse by criminals of consumer data that happens to be compromised through a data breach. Towards that end, payments technology businesses are bolstered by robust compliance practices—whether their own in-house policies, or ETA’s own carefully crafted industry Guidelines, which establish underwriting practices to help payments companies detect and eliminate fraud.

Importantly, for those companies that follow them, self-regulatory guidelines help ensure that consumer data is secure. The

Payment Card Industry Data Security Standard (PCI-DSS) created by the PCI Security Standards Council, is an example of one such successful industry-led, multi-stakeholder program, safeguarding personal information that should serve as a model. As a point of reference, fraud accounts for less than six cents of every one hundred dollars spent on the payments systems—a fraction of a tenth of a percent—and the payments industry is on the cutting edge of technology to help further limit fraud. But inasmuch as we just emerged from 2014, which the media dubbed “the year of the data breach,” the payments industry continues to innovate in order to further combat data breaches and protect consumers against increasingly sophisticated cyber criminals. It’s our highest priority, since our business depends on customers entrusting us with their personal and financial data.

An important step in this security upgrade is the transition to more secure chip, or “EMV,” cards, which use smart technology providing enhanced security.

ETA has long championed adoption of EMV enabled chip cards as one protection for consumers. EMV enabled chip cards, which can be identified by a conspicuous chip on the card’s face, currently only make up about 25% of total card circulation in the US, but this number is expected to increase to 90–95% within the next two years.

To incentivize more rapid migration to EMV adoption, just last week, on Oct. 1, the payments industry implement a long-planned liability shift for their card transactions, at which point any participant in the transaction chain who is not EMV compliant became responsible for any resulting fraud. This industry-led initiative is an example of how payments companies are proactively working to strengthen protection for consumers and the payments system.

To explain further, EMV, which stands for EuroPay, Mastercard, Visa, is the global standard for integrated circuit, or “chip” cards. Today, EMVCo (the body that sets that EMV specifications) is owned jointly by American Express, Discover, JCB, MasterCard, UnionPay, and Visa, and includes other organizations from the payments industry. EMV cards feature embedded microprocessor chips that store and protect cardholder data—similar to magstripe, but safer. An EMV card is superior to a traditional magstripe card because it supports dynamic authentication. EMV technology does this by generating a unique, or “dynamic,” one-time security code for each transaction, which makes the card nearly impossible to replicate. Counterfeiting such cards is currently far more difficult than producing cards with data that is “skimmed” from the magnetic stripes of genuine cards or stolen from stored payments data, such as the high-profile merchant breaches of recent months. Because EMV cards generate a dynamic security code with each transaction, unlike a magnetic stripe card which uses the same static code with every purchase, a counterfeit card could not successfully produce the correct security code and would not work in a card-present or face-to-face transaction. Accordingly, EMV is an effective tool to combat the manufacture and use of counterfeit cards and card-present fraud. Because counterfeit card represents

the single largest type of card fraud in stores in the U.S. today, the EMV migration is the most important step we can take. But although chip cards reduce the value of compromised data by inhibiting the creation of counterfeit cards, they do not stop data breaches. Later in my testimony, I will describe other initiatives within the industry that further augment the protections provided by EMV and will help erect additional barriers to bad actors, while simultaneously reducing the value of the data they may attempt to obtain.

Small Business Merchant Perspective

Of course, EMV-enabled cards are only half the EMV-migration equation, the other half is whether merchants have converted their point of sale terminals to accept them. Merchant acceptance of EMV cards is voluntary, and there are any number of factors facing individual small business merchants at this juncture which may affect their relative focus on, and timing for, their respective conversions. For instance, the cost of the conversion of terminals for the average small business merchant is in the \$50–\$500 range, and the cost and complexity vary depending on whether a small business merchant only needs to convert a single terminal, versus those with multiple terminals or terminals with integrated systems that combine payments functions with other functions, like inventory or payroll. For some, conversion to new EMV terminals may provide them an opportunity to upgrade to near field communication-enabled terminals in order to also be able to accept mobile payments, adding additional benefit for the merchant to convert sooner rather than later. In addition, there is a certification process all merchants must undertake in order to ensure compliance with card network rules and safeguards. On a much more practical level, we expect merchants right now are focusing on the upcoming holiday shopping season, but that migration efforts will really resume in 2016 after the holidays when many small business merchants renew their contracts with the card networks.

However, given that it was only last week that the official EMV liability shift happened, it appears as if the migration for some small business merchants will lag behind other businesses, especially if a small business merchant is the type where the likelihood of fraudster using a fraudulent card is low due to the low dollars involved in an average transaction—like at a dry cleaner or a car wash—and the resulting financial exposure to the merchant from the fraudulent transaction is, therefore, low. Put another way, a small business merchant may view the need to convert to EMV terminals—in order to avoid liability for a \$16 dry cleaning bill or a \$10 car wash paid for by a fraudulent card—as a relatively low priority. By contrast a small jeweler’s risk of liability for a fraudulently purchased \$6,000 diamond ring likely provides a greater incentive to convert to EMV terminals as soon as possible. Small businesses will make this risk/reward calculation, and this will cause variation amongst small business merchants in their respective EMV migration rates. At the end of the day, in the near term, the migration may require small business merchants to teach consumers how to check out with their newly-issued EMV cards in the

new point of sale terminals in order to keep customer transactions flowing smoothly, and this will take some effort on the merchant's part.

All of that said, there are any number of payments industry financial assistance and incentive programs to assist those merchants who may need it, and ETA has an educational website, www.sellSAFEinfo.org, to assist small business merchants with the EMV migration. Additionally, ETA's own Risk and Fraud Council recently published materials for small merchants to determine what they need to do when a breach occurs.

Finally, ETA is a participant in the PCI Security Standards Council Small Merchant Task Force. The goals and objectives of the task force are focused on ensuring that small merchants understand their responsibility for protecting payment card data and to identify and mitigate areas of risk in their environment. The payments industry has, and will continue, to educate and assist small business merchants in this regard.

EMV Chip and Cardholder Verification Methods

While this hearing specifically focuses on EMV, it is important to note that a separate question, independent of the EMV migration, has arisen regarding whether consumers should be required to use a personal identification number (PIN) for each credit card transaction at the point of sale. The EMV chip functions as a fraud prevention tool by generating a dynamic security code, thus preventing the production of counterfeit cards, the single largest (by far) cause of fraud in stores. Put another way, this ensures that the card itself is valid. The protection provided by EMV cards does not require a PIN. It is important to note that a PIN is a method of verifying the cardholder's identity (not that the card itself is valid, but rather that, in theory, the person presenting the card is the actual cardholder). This is referred to as a cardholder verification method, or CVM. A CVM prevents a specific type of card fraud called "lost and stolen" fraud—where a criminal has stolen a physical card from a wallet, for example, and then attempts to use the card before it has been reported stolen. Other methods of CVM include signature end, in some cases, no CVM is required, for example, because the transaction is a low dollar amount or low risk of fraud, and a CVM would not be beneficial to require.

ETA strongly supports the migration to EMV, and we believe that card issuers should be permitted to make the choice that is best for their customers as to cardholder verification method to accompany the chip cards, whether it be signature, PIN, or neither, when authorizing a transaction. Consumers and merchants have benefitted from flexibility in cardholder verification methods—including speedier checkout times for low dollar, low risk transactions. For example, drive throughs, quick service restaurants and convenience stores, in collaboration with payments companies and card networks, allow consumers to move quickly through checkout lines through "swipe and go" transactions that benefit all parties to the transaction and help maintain overall consumer satisfaction. Similarly, new mobile payments technology replaces traditional

CVMs with even more secure biometrics that promise both fraud protection and consumer convenience at a higher level. An important part of the decision of card issuers whether to require their customers to use a PIN is whether merchants have the capability to accept PIN as a CVM. It should be noted that, at present, roughly 2/3 of the nation's merchants do not have a PIN pad and thus cannot accept a PIN transaction from their customers. For such merchants, consumers who are required to use a PIN for a transaction could represent lost customers. It could also result in a shift of additional liability for fraudulent card transactions to those merchants that do not have a PIN pad.

Similarly, not all mobile payments can use a static PIN with the transaction. As merchants and consumers move from plastic cards to mobile devices, including mobile phones and wearables, this next generation of payments technology must not be inhibited by plastic card-era systems. Also, many consumers prefer not to have to remember PINs. Indeed, in 1967, the inventor of the ATM, John Shepherd-Barron, first envisioned a six-digit numeric code for customer authentication, but his spouse could only remember four digits, which became the commonly used length. Furthermore, the PIN is static and can be stored on a card, making it vulnerable to interception or even being guessed (there are only 10,000 possible 4 digit PIN combinations). As our industry moves to dynamic security, biometrics, and other systems that are even more secure, we must consider these important factors in making the right choice to secure transactions.

The fact remains that criminals are adaptive and constantly probe for vulnerabilities. Focusing on one specific technology gives hackers an open invitation to focus their energies on that technology and to detect and exploit loopholes in the payments system. Strong security involves a multi-layer approach which has the ability to evolve in response to the changing threat environment, allowing the industry to be as nimble as the bad actors it is attempting to thwart. At the end of the day, we all need to work continuously and collaboratively across banks, payments companies, merchants and consumers to find the most effective and efficient security mechanisms.

ETA Members: Fostering other new technology

As previously mentioned, EMV is one part of the overall, multi-layered solution to protecting data, consumers, and the payments system. ETA members are simultaneously deploying new innovations to further enhance security. For example, another technology, tokenization, removes sensitive information from a transaction by replacing customer data with a unique identifier that cannot be mathematically reversed. In its simplest form, it works like a secret code substituting symbols for important information like a credit card number. This way, only the bank that issued the card knows the real account information. Tokenization is designed to work when a consumer pays with plastic in person, online or with a mobile phone.

In a non-tokenized transaction, a consumer's actual account number is transmitted and, in some cases, stored by retailers, e.g, for purposes of facilitating returns. This trove of information is what hackers typically seek in the case of retailer data breaches. But in a tokenized environment, actual account numbers are replaced by one time-use tokens that represent account numbers but cannot be tied back to the actual number. If a breach occurs, the criminal only sees the tokenized code, which is useless to them because it cannot be used to generate a subsequent fraudulent transaction.

Another layer of protection deployed by ETA member companies is the use of point-to-point encryption. Point-to-point encryption is an advanced risk management tool that helps further protect data throughout the transaction lifecycle. With point-to-point encryption, card data is encrypted from the moment the card is swiped or tapped, while the data is in transit, all the way to authorization. This technology minimizes opportunities for hackers and criminals to access data during a purchase.

Additionally, many payment companies continue to innovate advanced computer systems that monitor transactions and data patterns detect unusual activity that may indicate an account has been hacked or a card lost or stolen. This monitoring occurs in both traditional, card-present as well as in card-not-present transactions, such as those taking place over the Internet or phone.

Lastly, using a mobile device to initiate a transaction may well be as common as swiping a card. Mobile payments and digital wallet cloud technology are actively employing new security technology that improves on legacy systems. Mobile devices provide enhanced security, including passcode protection for the phone, biometrics security features like a fingerprint, secure chip technology, geo-location information to assist with verification, as well as both device and cloud based encryption and tokenization capabilities.

The payments industry is creating innovative solutions today—like voice and facial recognition—to solve tomorrow's security threats. This protection ensures the flow of information vital to helping consumers access and use electronic payments, promotes competition and ensures the free flow of commerce, and maintains public confidence. It is imperative to find ways to encourage new technologies and enterprises, ensuring that the payments revolution will realize its maximum potential.

Conclusion:

Headline-grabbing events inevitably lead to calls for additional government regulations. The members of the ETA are the first line of defense for consumers to avoid the fraud perpetuated by criminals in the financial systems. As described, the payments industry takes seriously this charge and works hard every day to detect and deter crime. ETA members are deploying multiple layers of protection, including EMV, tokenization, encryption, biometrics, and other payments technologies that secure systems against criminal intrusions and protect consumers and merchants. As the trade association of the payments industry, ETA stands ready to assist the

Committee in its efforts to ensure that merchants, consumers and the economy continue to benefit from the safety and security of our nation's payments systems.



Testimony of

Paul Weston
Of
TCM Bank, NA
Tampa, FL

On behalf of the
Independent Community Bankers of America

Before the

United States House of Representatives
Committee on Small Business

Hearing on

**“The EMV Deadline and What It Means for Small
Businesses”**

October 7, 2015
Washington, D.C.

Chairman Chabot, Ranking Member Velazquez, and members of the committee, my name is Paul Weston, and I am President and CEO of TCM Bank, N.A. in Tampa, Florida. I testify today on behalf of the more than 6,000 community banks represented by the Independent Community Bankers of America (ICBA). Thank you for convening this hearing on the migration to EMV chip credit and debit card technology and what it means for small businesses. We're grateful to you for raising the profile of this important topic.

TCM Bank, N.A. is a \$178 million asset bank that serves as the credit card issuer and "back office" for over 650 community banks that have chosen to outsource the specialized function of credit card issuance. TCM Bank community bank clients brand and market their credit cards, expand their product offerings and customer relationships, and gain access to a new revenue stream, without committing financial, technical, or personnel resources to the day-to-day administration of a credit card program. This arrangement allows our community bank clients to focus on their core lending competencies: small business, consumer, and farm lending. TCM operates by the values and standards of service of our community bank clients.

The community bank business model is directly linked to the success of their small business customers. Community banks hold a disproportionate market share of small business loans—nearly 50 percent—though they hold less than 20 percent of all banking assets. ICBA and its community banks members take a keen interest in the migration to EMV chip cards, both as card issuers and as partners with the small businesses that are so important to the national economy. Locally-managed community banks are uniquely positioned to help small businesses make a smooth transition to EMV chip cards and are committed to doing so. TCM talks with community banks and their small business customers every day.

Before discussing in greater detail the ongoing migration to EMV chip and the respective roles of card issuers and merchants, I would like to stress that consumers—your constituents—are not on the hook for fraud losses as all credit cards have zero liability provisions for consumers and the Electronic Funds Transfer Act limits consumer liability for any fraud on debit cards. This is true whether or not the card issuer or the merchant is EMV chip compliant.

Small businesses that are involved with retail are already being presented with payment cards with an EMV chip on the front of the card in addition to the familiar magnetic stripe on the back of the card. In order to process those cards using EMV chip technology at the point of sale, most small business merchants will need to upgrade their terminals and train their front line staff to assist customers.

EMV chip cards contain a microprocessor that generates a unique, one-time code to authenticate card transactions. If the card information is stolen, it is useless to a criminal because it cannot be used to conduct another transaction. EMV chip cards are much more secure than magnetic stripe cards because they are exponentially more difficult to counterfeit. Counterfeit cards made with stolen information represent the largest portion of fraud in the United

States. And while consumers are protected against loss, having to replace a credit or debit card is inconvenient at best. EMV chip cards, together with merchant-provided chip readers at the point of sale, will play a critical role in reducing counterfeit fraud for both debit and credit cards.

Community banks are joining other financial institutions in the orderly migration to deploy EMV chip technology for debit and credit cards. This migration is already underway. A story in *USA Today* last week reported that roughly four in ten consumers already have an EMV chip card.

There is no legal mandate that card issuers adopt EMV chip or that retailers invest in EMV chip card readers. However, new rules in the card industry took effect on October 1, 2015 that will incentivize a shift to EMV chip technology that is in the best interest of all parties. The new rule provides that liability for fraudulent transactions sits with the party (i.e. retailer or bank) that didn't invest in chip technology. In a case where the bank doesn't offer chip cards and the merchant doesn't have a card reader, the bank will continue to be held responsible for covering the cost of the fraud. Similarly, in a case where both the bank and the merchant are chip compliant, the bank will continue to be responsible for losses incurred from fraudulent use. The October 1 liability shift represents a change in economic incentives rather than a legal mandate.

October 1 is not a *deadline* in any meaningful sense of the word. Instead the liability shift serves as a catalyst for change. Already, many card issuers and merchants have adopted EMV chip. Others will limit their liability exposure by adopting EMV chip before year-end. Some will choose to defer adoption into 2016 or even 2017 for automated fuel dispensers. Each issuing bank and each merchant will decide when to adopt EMV chip based on its own business model, vulnerability to fraud, and management of risk. The timing to complete each bank's reissuance of all cards in chip form will vary. Community banks will weigh the implementation and issuance costs with potential risk and demand from consumers. The migration to full EMV chip card usage will likely take several years to accomplish.

Based on many conversations with community banks and their small business customers, I believe that most small businesses are taking a very prudent approach to the migration. They are not buying from the first terminal salesperson who calls, and they are planning to closely follow as larger national retailers begin to enable EMV chip at the point of sale.

To give you a sense of what's involved for community banks, the initial costs of issuing EMV chip cards fall broadly into three categories:

1. *Card production and deployment*- Includes artwork and card redesign, acquiring new inventory of card stock, card personalization, and postage.

2. *Implementation*- Includes programming, software upgrades, processor costs, and new authorization techniques. ATMs and branch card issuance systems also need to be upgraded.

3. *Training*- All parties have to be trained. Community banks will focus on educating the cardholders as they adapt to a new way of presenting a card for payment at the point of sale in addition to training bank personnel and merchants to ensure that all parties can assist the consumer, even at the point of sale.

For merchants, the costs involve the purchase, deployment, and activation of EMV chip card readers. They must also train retail personnel to assist cardholders in the use of an EMV chip card. Community banks will serve as an important ally and resource to smaller retail businesses making the transition. They will help their merchant customers by providing equipment, expertise, and education to guide them through this change. Since community banks are local, they serve as “feet on the street,” especially for the small businesses in their communities.

For consumers, the transition will involve relearning a process which has become second nature. Instead of swiping a card through the magnetic stripe slot, a process that has become very well ingrained over many years, using an EMV chip card involves inserting the card into an open slot and leaving it there for a short time as the transaction is completed. Community banks are actively working to educate and reassure their customers about these changes coming to the point of sale.

While EMV chip cards are an effective means of reducing fraud related to counterfeit cards, they are not a panacea for all types of payment card fraud. Multiple layers of security technologies are needed in addition to EMV chip to mitigate other types of fraud. Card numbers and cardholder information must still be protected. The PCI Data Security Standards provide requirements for all merchants and processors to mitigate data breaches and compromise events that fuel payment card fraud. End-to-end encryption should be deployed to protect cardholder information while in transit, and newer technologies, such as tokenization, should and will be developed and deployed to protect online transactions.

Until this layered approach can be fully implemented, consumers should know that banks comply with significant legal and regulatory requirements and are subject to rigorous examination and supervision of their data security practices and procedures.

Some are touting PIN in combination with EMV chip as the only way to eliminate payments fraud. We believe any form of a PIN mandate would be misguided for a number of reasons. First, PINs only protect against fraud in cases of lost or stolen cards, which is a relatively small portion of total fraud. Second, as a static data element, PIN is more vulnerable than active technologies like EMV chip or tokenization. As PIN use becomes more prevalent, it attracts more criminal activity. A 2012 report by the Federal Reserve Bank of Atlanta found that debit PIN fraud rates have increased more than threefold since 2004.

Additionally, in order to better protect consumers, all participants of the payment system—including merchants—should be subject to the same federal data security standards and oversight as financial institutions. ICBA supports legislation introduced by Reps. Randy Neugebauer (R-TX) and John Carney (D-DE), the Data Security Act (H.R. 2205), that would apply Gramm-Leach-Bliley Act-like data security standards for all industries that handle sensitive financial information.

Closing

Thank you again for the opportunity to testify today. We hope that this hearing will help to educate all stakeholders, especially small businesses and consumers. The engagement and cooperation of all parties is critical for a smooth transition to EMV chip which will ultimately reduce fraud and bolster confidence in the payments system.



Testimony of

Jan N. Roche

President and CEO

State Department Federal Credit Union

on behalf of

The National Association of Federal Credit Unions

The EMV Deadline and What it Means for Small Businesses

Before the

House Small Business Committee

October 7, 2015

Introduction

Good morning, Chairman Chabot, Ranking Member Velázquez and Members of the Committee. My name is Jan Roche and I am testifying today on behalf of the National Association of Federal Credit Unions (NAFCU). I serve as the President and CEO of State Department Federal Credit Union (SDFCU), headquartered in Alexandria, Virginia, and also serve on the Board of Directors of NAFCU. I have over 30 years of experience in credit union and financial management.

State Department Federal Credit Union was chartered in 1935 through the efforts of eight employees of the Department of State. Now, 80 years later, we serve over 67,000 members worldwide and have over \$1.6 billion in assets. Due to the traveling habits and job assignments of many of our members and the fact that 8 percent of our membership is located overseas at any given time, we were one of the first financial institutions in the U.S. to start issuing EMV VISA Credit Cards in June, 2012.

As you are aware, NAFCU is the only national organization exclusively representing the federal interests of the nation's federally-insured credit unions. NAFCU-member credit unions collectively account for approximately 70 percent of the assets of all federal credit unions. We appreciate the opportunity to appear before you today to talk about the EMV transition deadline in the United States and the need for data security legislation, including H.R. 2205, the *Data Security Act of 2015*.

Background on Credit Unions

Historically, credit unions have served a unique function in the delivery of essential financial services to American consumers. Established by an Act of Congress in 1934, the federal credit union system was created, and has been recognized, as a way to promote thrift and to make financial services available to all Americans, many of whom may otherwise have limited access to financial services. Congress established credit unions as an alternative to banks and to meet a precise public need—a niche that credit unions still fill today.

Every credit union, regardless of size, is a cooperative institution organized “for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes.” (12 USC 1752(1)). While over 80 years have passed since the Federal Credit Union Act (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- credit unions remain wholly committed to providing their members with efficient, low-cost, personal financial services; and,
- credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

Credit unions are small businesses themselves, especially when compared to our nation's mega banks and largest retailers, facing challenges of meeting the products and service needs of their community, while dealing with various laws and regulations.

EMV

EMV is the established global standard for "chip" cards and their compatibility with point of sale terminals. EMV stands for "EuroPay, Mastercard and VISA," the three companies that created the standard. EMV cards are still plastic, but they contain an imbedded microprocessor (or "chip") that stores data and adds additional protection by making it harder to produce a counterfeit card that can be used at a point of sale terminal. This is because the chip generates unique data (a new, random number) for each transaction. If that data is stolen, it is not traceable back to the account. It is important to understand that it is this EMV "chip" technology that makes the new cards more secure—not a PIN or signature. It is also important to recognize that the EMV solution is the new market standard for combating fraud at the point-of-sale and assigning liability when a fraudulent credit card is used. It is not a "silver bullet" solution to the broader problem of data security or to combat online identity theft.

EMV is just one step in a larger universe of measures that credit unions take to protect the financial data of their members (consumers) and the payments system. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA) and are innovators in the ever-developing payments system as they strive to protect the financial information of the 101 million Americans who are credit union members.

My testimony today will cover how credit unions are protecting consumers in the payment system, the impact of the EMV transition and what steps are needed to better protect consumer financial data moving forward.

NAFCU's Work in Various Cyber and Data Security Initiatives

NAFCU is pleased to be an active participant in various industry and government payments, cyber and data security initiatives, doubling down these efforts as data breaches continue to rise and innovations in payments technology make the entire ecosystem more complex for financial institutions and consumers.

Specific to payments, NAFCU is a member of the *Payments Security Task Force*, a diverse group of participants in the payments industry that is driving a discussion relative to systems security. NAFCU also supports many of the ongoing efforts at the *Financial Services Sector Coordinating Council* (FSSCC) and the *Financial Services Information Sharing and Analysis Center* (FS-ISAC). These organizations work closely with partners throughout the government creating unique information sharing relationships that allow threat information to be distributed in a timely manner.

NAFCU also worked with the *National Institute of Standards and Technology* (NIST) on the voluntary cybersecurity framework released in 2013 designed to help guide financial institutions of varying size and complexity through the process of reducing cyber risks to critical infrastructure. The recommendations are designed to evolve and will be updated to keep pace with changes in technology and threats.

Earlier this year, NAFCU also participated in President Barack Obama's *White House Summit on Cybersecurity and Consumer Protection* at Stanford University which featured leaders from across the country—industry, tech companies, law enforcement, consumer and privacy advocates, law professors who specialize in this field, and students—to collaborate and explore partnerships that will help develop the best ways to bolster cybersecurity. Credit unions continue to pursue greater data security through innovation.

During the Summit, NAFCU-member First Tech Federal Credit Union's recent partnership with MasterCard in the area of card security was announced. First Tech is innovative in this area and is implementing a new pilot program this year that will allow consumers to authenticate and verify their transactions using a combination of unique biometrics such as facial and voice recognition. This type of innovation is a generation beyond EMV, and is not unusual at member-owned and member-driven credit unions as we take data security seriously. Technological innovations like this are a prime example of why Congress needs to ignore calls to legislate technological solutions, which can soon become out-of-date, rather than creating basic standards of data protection.

NAFCU is also a participant in the Federal Reserve's initiative to improve the U.S. payments systems through two industry taskforces launched earlier this year: the Faster Payments Taskforce and the Secure Payments Taskforce. Through the Faster Payments Taskforce, NAFCU is working with the Federal Reserve and industry participants to create criteria to identify and evaluate alternative approaches for implementing safe, ubiquitous, faster payment capabilities. Additionally, on the Secure Payments Task Force, NAFCU is providing input to the Federal Reserve on payment security matters and is helping determine priorities for future action to advance payment system safety, security and resiliency.

The EMV Transition

October 1, 2015, was the deadline established by the four major U.S. credit card issuers (Mastercard, Visa, Discover and American Express) when the liability for the majority of card-present fraudulent transactions on credit cards is shifted to whichever party is not EMV-compliant. Given the nature of our field of membership, which includes many State Department employees that travel or are stationed overseas in countries where the EMV transition has already occurred, SDFCU was an early adapter to the U.S. transition, first issuing EMV cards in June of 2012 for new cards and replacements for lost and stolen cards. Our credit card portfolio of over 28,000 cards is now 100% EMV.

It is important to note that the EMV transition in the U.S. is a voluntary one established by the market, and not a government mandate. The October 1, 2015, deadline is not the endpoint of transition, rather just a step along the road of progress when the incentives to be EMV-compliant changed. Companies have not been forced to transition (whether it's issuing or accepting EMV cards) if they are willing to bear the liability. The speed of shifting to EMV is essentially a business decision that is dependent on risk-tolerance. It is important to note that, whether or not a card or business is EMV-compliant, consumers are not liable for fraud losses as all credit cards have zero liability provisions for consumers and the *Electronic Funds Transfer Act* limits consumer liability for any fraud on debit cards. Consumers remain protected in the new system.

Based on a NAFCU survey of our members, a majority of credit unions are ready for the EMV transition and are issuing EMV credit cards to their members as they issue new cards or replace older magnetic-stripe cards. There is a greater cost for an EMV card for credit unions. At SDFCU, the cost (not including staff costs, set up and postage) to produce a non-EMV card is approximately \$3.04 and to produce a new EMV card it is approximately \$5.81.

A comprehensive study released September 17, 2015, by the Strawhecker Group reported that only 27% of merchants were to be EMV-ready by October 1, 2015. In other recent surveys, the reasons given by merchants for not being ready include: not knowing about the transition (despite it being several years in the works), not wanting to pay for an EMV terminal, not being concerned about the liability shift and thinking that the EMV shift is unfair. Many of these are small and mid-size businesses that could find themselves the next targets of data thieves that will seek to exploit this vulnerability in the payment system as many big box retailers make the conversion. We believe that successful protection of the payments system requires all parties to be actively involved and hope that these businesses will work with the financial services community to recognize their role in making the payments system safer.

The PIN Debate

Some have argued that the EMV transition should have included a PIN mandate to require consumers to enter PINs for every transaction. Imposing such a mandate or requirement would be unrealistic and would not be a panacea for the problem of data security. As I noted earlier, it is the chip technology that makes new cards secure, not the PIN or signature. A PIN is a static data element that is still vulnerable to theft. If it is compromised, a consumer's entire account can be put at risk. A 2012 report by the Federal Reserve Bank of Atlanta found that PIN fraud rates had increased significantly since 2004. A PIN mandate would not have helped prevent recent major consumer data breaches such as Target, Home Depot and Michaels.

A PIN mandate also does not prevent online or mobile fraud, often referred to as “card-not-present” fraud, which is already 45% of card fraud in the U.S. according to the Aite Group (at SDFCU in the last year, it was about 40% of our gross card fraud). This type of fraud is also expected to rise significantly after the EMV transition. Wider use of PINs in other EMV countries have done nothing to prevent spikes in card-not-present fraud. In the United Kingdom, online fraud rose 79% after their EMV transition. In Canada, while card-present fraud declined after the switch to EMV, card-not-present fraud more than doubled.

A truly secure payments system must be one that is constantly evolving to meet emerging threats and uses a wide range of dynamic authentication technologies—EMV, tokenization, encryption, biometrics and more. Many retailers today are increasingly moving away from traditional point-of-sale authentication methods, like PIN or signature, and relying on network-based monitoring to identify fraud as it can improve the customer experience by reducing time spent in the checkout line. Many of you may have experienced transactions where the merchant does not request a signature nor PIN with card usage. Retailers have demanded this change of the industry to speed the checkout process. Because retailers do not have standards requiring them to protect consumer data collected at the point of sale, they have sometimes prioritized the speed of the transaction to increase customer sales at the expense of the security of the payment system. This can make retailers a vulnerable point of entry to data breaches in the payments ecosystem, even with PIN and signature authentication.

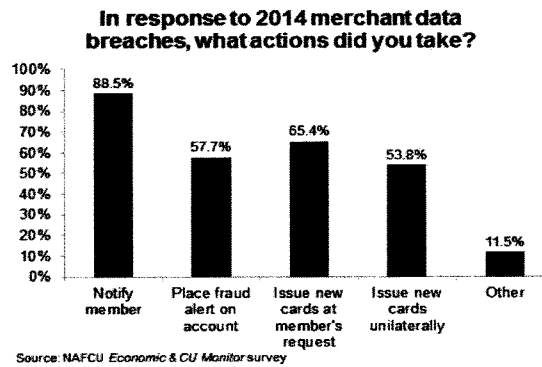
Credit Unions and Consumers Suffer in Data Breaches

The EMV transition is not a silver bullet to addressing the scourge of data breaches. More needs to be done to establish a national standard for protecting the financial data of consumers. Americans are becoming more aware and more concerned about data security and its impact. A Gallup poll from October, 2014, found that 69 percent of U.S. adults said they frequently or occasionally are concerned about having their credit card information stolen by hackers, while 27 percent of Americans say they or another household member had information from a credit card used at a store stolen in the last year. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

Data security breaches are more than just an inconvenience to consumers as they wait for their plastic cards to be reissued. Breaches often result in compromised card information leading to fraud losses, unnecessarily damaged credit ratings, and even identity theft. Symantec’s *Internet Security Threat Report* issued earlier this year found that 36% (roughly 74 million consumers) of the over 205 million individuals compromised in retail breaches in 2014 had their financial information exposed. That percentage doubled from 18% in 2013. More than 23% of the US population had their financial identities compromised by a retailer data breach in 2014.

While the headline grabbing breaches are certainly noteworthy, the simple fact is that data security breaches at our nation's retailers are happening almost every day. A survey of NAFCU member credit unions, found that respondents were alerted to potential breaches an average of 164 times in 2014. Two-thirds of the respondents said that they saw an increase in these alerts from 2013. When credit unions are alerted to breaches, they take action to respond to protect

their members. The chart below outlines the actions that credit unions took in 2014 in response to merchant data breaches.



Merchants and credit unions are both targets of cyberattacks. The difference, however, is that credit unions have developed and maintain robust internal protections to combat these attacks and are required by federal law and regulation to protect this information and notify consumers when a breach occurs that will put them at risk. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to \$1 million per day for compliance violations. In contrast, retailers are not covered by *any* federal laws or regulations that require them to protect the data and notify consumers when it is breached.

Credit Unions and GLBA

As I noted above, credit unions, and all financial institutions, are subject to the 1999 *Gramm-Leach-Bliley Act*, GLBA and its implementing regulations have successfully limited data breaches among financial institutions and this standard has a proven track record of success since its enactment. This record of success is why we believe any future requirements must recognize and incorporate this

existing national standard for financial institutions such as credit unions.

Consistent with Section 501 of the GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLBA and its implementing regulations have successfully limited data breaches among credit unions. NAFCU believes that the best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

There are a number of key elements, requirements and definitions of the GLBA that apply to credit unions and are outlined below. The GLBA directed regulators to establish evolving standards for financial institutions to ensure the security and confidentiality of consumer information.

The GLBA also sets a number of important definitions and requirements:

Sensitive Consumer Information

Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log into or access the member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

Unauthorized Access to Consumer Information

The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or

use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

Risk Assessment and Controls

The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business. This is a critical aspect of GLBA that allows flexibility and ensures the regulatory framework is workable for the largest and smallest in the financial services arena. As the committee considers cyber and data security measures, it should be noted that scalability is achievable and that it is a misnomer when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying size businesses.

At a minimum, the credit union is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing consumer information to authorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to consumer information;
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information sys-

tems, including appropriate reports to regulatory and law enforcement agencies;

- Train staff to implement the credit union's information security program; and,
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."

Service Providers

The security guidelines direct every financial institution to require its service providers through contract to implement appropriate measures designed to protect against unauthorized access to, or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events, costs savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

An institution that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

Response Program

Every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. **The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.**

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers. Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

Consumer Notice

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good con-

sumer relations, and enable the institution's members to take steps to protect themselves against the consequences of identity theft.

Content of Consumer Notice

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected fraud or identity theft to the institution.

Delivery of Consumer Notice

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

Preventing Future Breaches

While financial institutions are subject to the robust standards of the GLBA outlined above, retailers and others who handle financial data are not subject to the same type of national standard. NAFCU has long argued that protecting consumers and financial institutions by preventing future data breaches hinges on establishment of strong federal data safekeeping standards for retailers and merchants akin to what credit unions already comply with under the GLBA. NAFCU has developed a number of key principles that should be considered and incorporated in the data security debate (Appendix A). Unfortunately, merchants have attempted to use the EMV and PIN debate to stop any meaningful discussion about data security legislation—thus not addressing the real issue of the broader responsibility of merchants to protect consumers' financial data.

The time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Such a standard must recognize the existing protection standards that financial institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach.

While some have said that voluntary industry standards should be the solution, the recently released *Verizon 2015 Payment Card Industry Compliance Report* found that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. In fact, Verizon found that out of every data breach they studied over the past 10 years, not one single company was in compliance with the PCI standards at the time of the breach. This should cause serious pause among lawmakers as failing to meet these standards, exacerbated by the lack of a strong federal data safekeeping standard, leaves merchants, and therefore consumers, more vulnerable to breaches.

One basic but important concept to point out with regard to almost all cyber and data threats is that a breach may never come to fruition if any entity handling sensitive information limits the amount of data collected on the front end and is diligent in not storing sensitive personal and financial data in their systems. Enforcement of prohibition on data retention cannot be over emphasized and it is a cost effective and commonsense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of cyber criminals.

Legislative Solutions

NAFCU believes that the best legislative solution on the issue of data security that has been introduced in this Congress is the bipartisan legislation introduced by Representatives Randy Neugebauer and John Carney, H.R. 2205, the *Data Security Act of 2015*. This legislation creates a national data security standard that is flexible and scalable, does not mandate static technology solutions and recognizes those who already have a working standard under the GLBA. We support this legislation and would urge you to support it as well.

Conclusion

Cyber and data security, ensuring member safety, and incentivizing data safekeeping in every link of the payments chain is a top challenge facing the credit union industry today. A truly secure payments system must be one that is constantly evolving to meet emerging threats and uses a wide range of dynamic authentication technologies—EMV, tokenization, encryption, biometrics and more. When it comes to EMV, what matters most is the chip technology that makes the cards more secure. Requiring additional measures such as PIN usage does not make substantial improvements to the system. While credit unions are largely ready for the EMV transition, wider adoption of EMV technology by others in the payment system, such as retailers, will only strengthen the system. Still, more needs to be done.

Consumers will only be protected when every sector of industry is subject to robust federal data safekeeping standards that are enforced by corresponding regulatory agencies. It is with this in mind that NAFCU urges Congress to modernize data security laws to reflect the complexity of the current environment and insist that retailers and merchants adhere to a strong federal standard in this regard. Enacting H.R. 2205, the *Data Security Act of 2015*, would be an important step toward this goal.

Thank you for the opportunity to appear before you today on behalf of NAFCU. I welcome any questions you may have.

Appendix A

NAFCU's Key Data Security Principles

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *GLBA*.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer

who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

October 7, 2015

Statement for the Record
Of the
American Bankers Association
before the
Committee on Small Business
United States House of Representatives



Statement for the Record
American Bankers Association
Committee on Small Business
United States House of Representatives
October 7, 2015

The members of the American Bankers Association, who serve small businesses across the Nation, deeply appreciate Chairman Chabot's and Ranking Member Velazquez's decision to hold this important hearing on the EMV chip card upgrade. The ABA is the voice of the nation's \$15 trillion banking industry, which is composed of small, mid-size, regional and large banks that together employ more than 2 million people, safeguard \$12 trillion in deposits and extend more than \$8 trillion in loans.

Every day, ABA's thousands of members, found primarily on the Main Streets of America, have the privilege to work with the millions of American small businesses who form the bedrock of our economy. Most banks are small businesses themselves, with the median sized-bank having 42 employees and four branches. In fact, the Small Business Administration considers 80 percent of banks to be small businesses. Providing small businesses with credit and payment services is the bread and butter of banking.

As the Committee is aware, the banking industry is leading a major payment card security upgrade, with "EMV" credit and debit chip cards being issued to protect consumers and brick-and-mortar merchants from criminals who engage in card counterfeiting.¹ This change is all about security—the chips are almost impossible to copy or counterfeit. Banks have been moving quickly to put this security upgrade into consumers' wallets. Most people have at least one chip card in their wallet now, and we estimate that 575 million chip cards will have been issued by the end of 2015.

Consumers will start seeing more point-of-sale terminals that are ready to accept their chip cards. This is critical, of course, as the benefit of this advanced chip technology can only be realized if merchants have chip-card readers in their stores. This will be a gradual process—which really began in 2011 with the announcement of the move to EMV in the U.S.—but the incentives changed on October 1 to encourage both banks and merchants to adopt the new advanced EMV standard as soon as possible. Whichever party has not updated to the EMV standard would be liable for any fraud losses. This was not a government mandate, nor a deadline, but rather a private sector joint effort—banks, networks, and merchants—to enhance payment security for all our customers.

Banks have worked closely with small businesses throughout this upgrade process to ensure that they are prepared. Several

¹ EMV stands for "Europay, MasterCard, Visa," which were the original chip developers, but chip cards can be used on all major U.S. card networks, including American Express, Discover, MasterCard, and Visa.

banks and merchant services companies have offered incentives to offset costs involved in upgrading terminals, making them free in some cases.

Since this is a gradual process, consumers do not have to worry about their current card being accepted after October 1—their chip card will still have a magnetic stripe that will work at stores without a chip terminal. It is also important to emphasize that consumers will continue to enjoy the same protections for fraud—zero liability in most cases.

EMV chips are an important innovation that better protect consumers' financial data, but they are part of the greater effort being made by banks and networks to combat hackers. Other innovations are on the horizon and will play an important role fighting future threats. Tokenization technologies that replace account numbers with a random number at the point of purchase rendering them useless to thieves (like Apple Pay and Samsung Pay) are becoming more common. Point-to-point encryption scrambles data at every point of the transaction. In addition to today's sophisticated neural networks which spot fraud at the point of sale, these new technologies will be layered on top of EMV and create multiple dynamic layers of security necessary to fight increasingly sophisticated forms of fraud. We do not know what thieves might do next, which is why dynamic security features are so critical and why mandating a static technology approach to security (such as Personal Identification Numbers, PINs), as some advocate, is a mistake.

There are three key points we would like to make in the remainder of this statement:

- > Banks are committed to secure payment solutions for small businesses;
- > EMV chip cards confront counterfeit card fraud, helping customers, merchants and banks; and
- > Banks and small businesses must partner to assure a safe payment system for our customers.

I. Banks are Committed to Secure Payment Solutions for Small Businesses

Banks have always acted as a trusted payment intermediary, facilitating confidence in commerce. Unlike much of the world (including most of Europe), the United States has benefited from a truly network-based, electronic payment card system for many decades. While these other countries were still developing the telecom infrastructure to support real-time card payments, Americans were able to have transactions authorized in seconds. Fortunately, this real-time card technology has largely become the global standard. That adoption speaks to the leadership role that American banks, networks, and others play in providing the most secure and reliable solutions to our customers. We understand the seriousness of this trust to operate a payment system that is transparent, efficient, and most importantly, *secure* for all participants.

Banks are committed to protecting small businesses from fraud. When payment fraud occurs, there are three parties who are indis-

putable victims of crime: consumers, merchants, and financial institutions. We all share the sense of violation when a credit or debit card is misused by thieves intent on obtaining ill-gotten gains. In a world where criminals are working full-time to steal from consumers, it falls upon financial institutions to be sentinels of the consumer's financial security. It is often a banker who takes the first call in these situations, and usually the banker who must relay the news to a card customer that they also have been a victim of a crime. Many times, ABA's members detect and stop these crimes in progress.

ABA's members accept this duty and demonstrate it by investing billions of dollars a year in security measures, and by making consumers whole through no-hassle liability protection policies that almost always exceed legal requirements. In an era where criminals are constantly changing their tactics, the payments industry is not sitting still.

II. EMV Chip Cards Confront Counterfeit Card Fraud

Despite all this progress, there has been an uptick in a certain kind of fraud, known as card counterfeiting, which makes up the vast majority of in-person card fraud today. As its name implies, card counterfeiting involves creating a fake card using information gleaned from a real card.

It used to be that counterfeit cards were made from criminals using skimmers to strip the data from the magnetic strip ("magstripe") and make duplicate cards—a very labor-intensive process. Criminals, like water, always seek paths of less resistance, which is why a second route of counterfeit fraud is increasingly important: big retailer data breaches. The prospect of being able to access millions of card numbers at once, from a great distance away, makes hacking into retailers' systems their new preferred way to steal customer information.

Recent high-profile data breaches at retailers like Target and Home Depot underscore the critical need for stronger and more innovative security solutions that protect consumers. The damage done by these breaches is well-known and affected perhaps more victims than any other financial crime in American history.

In the wake of these breaches, card-issuing banks made consumers whole quickly, often wiping fraudulent charges off their account immediately upon being notified. Through proactive steps on the part of banks, most affected customers did not see any fraudulent activity, although the disruption of card reissuance was real for both consumers and businesses.

These high-profile retail breaches added urgency to the efforts already underway to fight counterfeit fraud that would make it harder to monetize stolen card data. Moving from the magstripe (which stores *unencrypted* information) to the EMV standard was one of those, and that process had begun in earnest in 2011 in the U.S. Some have questioned why the U.S. was slower than Europe to adopt chip technology. The answer lies in the fact that EMV was originally designed to solve a European payments problem: Europe

lacked the advanced telecom infrastructure that was allowing U.S. retailers to authorize card transactions in real time.

While American businesses routinely sent card information across phone lines to obtain authorization from card-issuing banks, European retailers found telecom rates too expensive to make a call for every transaction. The solution was to issue Europeans cards with microchips which contained information like credit limits and fraud indicators, which would have been kept on the issuing bank's computer in the U.S. system. Instead of processing transactions "over the wires" (as in the U.S.) EMV chips and terminals allowed European card transactions to be processed without an immediate connection to the payment network. Transaction data would be stored in the terminal until the merchant terminal contacted the bank to settle the day's transactions.

This "offline" approach had obvious limitations (mainly that transactions were not checked through a central system at each sale) and disadvantages compared to the U.S. system of live authorizations. Fortunately, these European systems have been upgraded over the years.

In contrast, the U.S. EMV introduction combines the security benefits of EMV chips and the real-time authorization of transactions through the bank's computers. From the outset, EMV chips in the U.S. are running software that produces a one-time code which is sent across the network during each transaction and is required for authorization by the bank computer on the other end. Neural network and live authorizations, which spot and shut down suspicious transactions, form the basis for dynamic security for U.S. transactions. A crucial distinction is that EMV chip cards' anti-counterfeiting properties are found in the chip itself and are unrelated to the use of a Personal Identification Number (PIN). Simply put, the chip is what makes the difference, not a PIN.

The EMV chip that was built to meet the challenge is serious security equipment. For starters, the chips are inherently counterfeit-resistant hardware, making it virtually impossible to create a fake chip. A core security feature of EMV is a one-time, non-reusable code that the chip produces for each transaction. Called a "cryptogram," this code is the result of advanced mathematical algorithms which cannot be entirely observed by hackers. The code can only be used once, so it is useless for future transactions if stolen. If a criminal attempts to use the code, the payment systems will recognize that it has already been used and will not authorize the transaction. This one-time code is an additional layer of security that rides on top of other card data.

The "Liability Shift" Gives Banks and Merchants Incentives to Employ the Best Technology

In 2011, one of the card payment networks announced that it would begin supporting EMV in the U.S. This was a major step in combatting counterfeit fraud. However, this upgrade would not happen overnight. Of course, banks would have to issue hundreds of millions of new cards, at several times the price of magstripe cards. Card-accepting businesses would incur costs and require

transition time as well. EMV cards can only be read by EMV-enabled terminals (“dipping” the card and letting it stay in a terminal through the entire transaction replaces “swiping” a magstripe).

That network set October 1, 2015 as the date on which merchant or bank liability for fraudulent counterfeit transactions would depend on whether either party was using EMV technology. ATMs and gas stations were given later incentive dates, to allow their owners more time to address technical issues which are specific to those applications.

This “liability shift” has sometimes been mischaracterized and we want to ensure that the Committee has an accurate understanding of what it means. Today banks absorb less from in-person use of counterfeit cards at merchants. After October 1, 2015, banks will still absorb these losses if a counterfeit card of any kind is used at an EMV-enabled merchant. This includes magstripe cards used at an EMV-enabled merchant. Simply put, if the merchant has upgraded to an EMV-enabled terminal and is using it, nothing changes for them—the issuing bank will still be liable. However, if the bank has issued an EMV card and the merchant does not have a terminal to accept the chip (forcing consumers to use the more easily counterfeited magstripe part of the card), the merchant is liable for the resulting fraud, because they have failed to use the latest technology available to them.

The October 1, 2015 date was a private sector incentive to get consumers protected as soon as possible. It was most certainly not a “deadline” or government mandate. Small businesses which did not accept EMV cards on that day did not see their card terminals turned off or see the experience change for their customers. It was a contractual change that only became relevant in the case of criminals using counterfeit cards.

It is important to note that the security benefits of EMV deployment in the U.S. are more powerful than in the original introductions of the technology in other countries. Since U.S. cardholders already conduct real time transactions, they are already protected by a complex series of seen and unseen security systems (including neural networks which spot and shut down suspicious transactions). The EMV chip technology is another layer that fits in well with these other measures. The EMV chips used in the U.S. contain security software, which work with the security systems at the payment network and issuing bank to further protect transactions. The microprocessor in the chip can run this software whenever a transaction occurs. These security checks happen in the background, sometimes triggering a “pause” in the transaction to obtain further verification from the person presenting the card. The EMV chip is built on a flexible standard, which is also capable of facilitating data encryption and can be customized for emerging security paradigms.

By deploying EMV cards in the U.S. and combining this chip technology with the real-time transaction capabilities which Americans are used to, the payment industry was able to leverage more than the original security features of EMV. Not only do American consumers benefit from a card that is difficult to counterfeit, but

transactions are also protected by cutting-edge fraud prevention measures.

III. Banks and Businesses Must Partner to Ensure a Safe Payment System for Our Customers

From the beginning of the EMV upgrade effort in 2011, the financial services sector has been focused on ensuring that the upgrade would be accessible to small businesses. Recognizing that there are costs involved, several banks and merchant services companies have incentives to upgrade terminals, making them free in some cases. These free terminals are often provided in the context of an ongoing relationship between the merchant and a payment services company. Many terminals have been “turned over” into EMV terminals during routine register hardware changes, meaning little to no marginal costs to merchants to upgrade. Payment services companies have proactively engaged their business customers to inform them about the October 1, 2015 incentive date and offer hardware and software solutions to help them become part of the upgrade. An “in the market” survey of options available in the market demonstrates that a basic terminal can be obtained for about \$200 and more sophisticated systems cost a few hundred dollars more, but include helpful features like inventory tracking and customer relationship features, which many retailers will find useful. For mobile merchants or those using tablet-computer based points of sale, Square sells an EMV-reading accessory that cost \$29.

This upgrade is also an opportunity for many businesses to grow their acceptance of emerging payments which consumers are demanding. Although not mandatory, EMV terminals which come equipped with NFC (“near field contactless”) capabilities provide a shorter route to accepting Apple Pay, Samsung Pay and similar mobile wallets. Some of these ancillary options contain powerful security mechanisms like “tokenization” and strong encryption. These newer terminals also have upgradable software, meaning that merchants can likely “keep up” with consumer trends for several years before having to upgrade again. These are all choices that merchants can make with the help of their merchant services company. It all means that EMV upgrades at the register are the gateway to the future of payments.

This dynamic, open approach to payment innovations is the vision that the banking industry has for the future of payment security. Fortunately, the global EMV standard has shown itself to be flexible enough to be adapted from the chip to mobile devices.

Although news coverage may focus most on how businesses *accept* chip cards, we must remember that businesses are also cardholders themselves. They deserve payment cards that are reliable and safe. As the EMV upgrade progresses, businesses that use credit cards for purchases will likely find that fraud-related card deactivations and reissuances become rarer. This will eliminate disruptions to business operations for the large number of firms that have turned to card payments as a way to manage risk and streamline purchasing.

Conclusion

The banking industry continues to take its role as sentinel of consumer payments seriously. Importantly, we recognize that payments are only secure when all stakeholders guard data and participate in the upgrades that are developed to protect consumers. Every day, Americans are receiving new chip cards in the mail and retailers are plugging in their new terminals (or attaching them to their mobile phones). EMV is gradually becoming a way of life for shoppers and its security benefits are being realized more with each passing day. Soon, using EMV cards will be second nature for consumers, and we fully expect that small businesses will be able to claim a large share of the credit for making this transition successful.

But EMV is not the endpoint of card security, no more than physical cards are the endpoint for payments. Like the many cumulative measures introduced before EMV, this technology is one more layer of protection introduced in a long line of security upgrades. In a world of emerging security threats, there is always more that can be done to protect consumer payment information. This is why banks continue to urge large retailers to upgrade their data security to match the levels that our industry must meet under federal law.

For our part, banks will continue to innovate to put criminals on the defensive and protect legitimate commercial actors, including small businesses. In the battle against modern criminals, the EMV upgrade continues to be an opportunity for a positive story about collaboration between America's small businesses and the bankers who have the privilege to serve them.

**STATEMENT FOR THE RECORD
BY LYLE BECKWITH
ON BEHALF OF
THE NATIONAL ASSOCIATION OF CONVENIENCE
STORES
FOR THE
HEARING OF THE HOUSE SMALL BUSINESS COMMITTEE
OCTOBER 7, 2015
“THE EMV DEADLINE AND WHAT IT MEANS FOR SMALL
BUSINESSES”**

My name is Lyle Beckwith. I am the Senior Vice President, Government Relations for the National Association of Convenience Stores (NACS) and I appreciate this opportunity to present NACS' views regarding the implications of the EMV chip deadline for small businesses.

NACS is an international trade association representing more than 2,200 retail and 1,800 supplier company members in the convenience and petroleum retailing industry. NACS member companies do business in nearly 50 countries worldwide, with the majority of members based in the United States. In 2014, the industry employed more than two million workers and generated \$696.1 billion in total sales, representing approximately 4.0 percent of the United States' GDP—or one of every 25 dollars spent. The majority of the industry are small, independent operators. More than 70 percent of the industry is composed of companies that operate ten stores or fewer, and 63 percent of them operate a single store.

The process of transitioning to EMV—a process dictated by the major card companies without input from retailers, consumers, or banks—has been and will continue to be onerous and very expensive for merchants. On top of that, the full security and consumer protection benefits of the transition will not be realized. By the card companies' choice—and unlike what has been done in other parts of the world—Visa and MasterCard are having the U.S. transition to chip technology without the use of Personal Identification Numbers (“PIN”), rather than the chip-and-PIN technology that has a proven track record of success. Below we offer more detailed comments on the transition, its impact on small businesses, and the lost opportunity for substantially reducing fraud in the payment card system.

I. The card companies' justification for this mandatory transition is flawed.

Beginning October 1, 2015, any merchant that is not equipped and certified by the major card companies to accept EMV or “chip” cards will have liability for fraudulent credit and debit card transactions involving chip-embedded cards. The card companies claim they are requiring merchants to transition to EMV to increase security in card transactions, and so they and the banks will no longer have to pay for losses caused by fraud. This rationale does not make sense for multiple reasons.

First, *merchants* pay for the majority of fraud losses today, not card companies or banks.

Second, the card companies have intentionally chosen not to transition to the most secure payment method available. If the card companies were legitimately interested in minimizing fraud losses, they would require chip *and* PIN, not just chip (as discussed in further detail below).

And third, the card companies themselves, not merchants, have delayed bringing new technologies and security measures to the U.S. payment card industry.

Notwithstanding the foregoing, NACS strongly believes that something must be done to reduce fraudulent transactions. Our commitment to improving card security stems from the fact that merchants currently pay the majority of fraud costs, which are spiraling out of control. In 2014, global credit and debit card fraud topped \$16.3 billion across all industries—\$7.6 billion of that fraud occurred in the U.S.¹ Despite banks' claims that they provide a "payment guarantee," merchants are absorbing the vast majority of the costs associated with fraudulent transactions.²

While chip-embedded cards are harder to counterfeit or copy, without a PIN number, they do not help reduce many types of fraud. For example, chip cards and card numbers can still be stolen and used by someone who is not the account holder. Stolen chip card numbers can be used online. And counterfeit chip cards can still be made, but when someone presents a card with a non-functioning chip, the card's magnetic stripe will be used or the card's number will be entered to complete the fraudulent transaction. Requiring PIN would help in all of these scenarios. Simply put, chip without PIN is not enough.

The fraud-reduction benefits of requiring chip *and* PIN—or even just PIN on old magnetic strip technology—are far greater than requiring chip alone. It is no wonder that chip and PIN technology has been the standard in Europe for almost 20 years; or that the technology is already used in virtually every other industrialized country. Use of outdated magnetic strip technology in the U.S. has been the only option because the *card companies* have not, until now, provided chip and PIN in this market, despite the urging of retailers, consumer advocates, and cyber security experts.

Thus, before considering the cost to small businesses of completing the mandatory transition to EMV, it is worth questioning the card companies' justification and motivation for this particular mandate. For instance, it is worth asking: why mandate the transition to EMV—with all of its attendant effort and cost—without requiring PIN? Why would anyone choose not to maximize fraud prevention benefits with this costly transition? And why, after years of delay in bringing EMV capability to the U.S. market, impose an arbitrary and inflexible deadline on merchants, despite implementation challenges beyond their control?

II. The transition is costly for merchants and especially difficult for small businesses to implement.

The cost to businesses to become EMV-ready is substantial. There are approximately 152,000 convenience stores in the U.S. and it will cost approximately \$3.9 billion—\$26,000 per store—to

¹ Skowronski, Jeanine, *US coming back to credit cards*, Bankrate (May 28, 2015), available at <http://www.bankrate.com/financing/credit-cards/u-s-coming-back-to-credit-cards/>; see also, *Global Card Fraud Losses Reach \$16.31 Billion—Will Exceed \$35 Billion in 2020 According to The Nilson Report*, Business Wire (Aug. 4, 2015), available at <http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VgGWMd9VhBc>.

² Press Release: *U.S. Retailers Face \$191 Billion in Fraud Losses Each Year*, LexisNexis Risk Solutions (Nov. 9, 2009) (highlighting findings of LexisNexis and Javelin Strategy & Research "True Cost of Fraud Benchmark Study"), available at <http://www.lexisnexis.com/risk/newsevents/press-release.aspx?Id=1258571377346174>; "House of Cards: Why your accounts are vulnerable to thieves," Consumer Reports, June 2011.

make them EMV capable. To put those figures in perspective, about 60 percent of convenience stores belong to single-store owner/operators and the average profits for a convenience store per year are \$47,000. So the initial upfront cost—not even counting future maintenance and update costs—is more than half of an average store’s profits. On top of that, on-going maintenance and upgrade expenses are expected to be upward of \$2,240 per year, per store.

The transition to EMV necessitates the purchase by merchants of specialized hardware and software, along with numerous other steps. According to one survey of U.S. retailers, ordering new terminals can take 6 to 16 weeks. Then retailers and payment card processors must program the new equipment according to card company specifications, which can take months. In fact, it has been very difficult for small businesses to get the programming help they need given the high demand for these services. Notably, the card networks did not release the debit specifications necessary to program terminals to accept those cards until March 2015. That delay did not leave enough time for many merchants to program their systems and accept EMV by October 1st, and it added to the bottle-neck of demand for programming services.

Following the programming phase, retailers must conduct internal testing and trouble-shooting, and then obtain certification by the card companies. Visa, MasterCard, American Express and Discover each require a *separate* certification. On top of that, separate certifications are required for credit, PIN debit, and signature debt. This has been another source of delay—particularly for small businesses. The card networks simply have not deployed the resources necessary to get merchants that want EMV operating on time. Finally, after the new technology is certified, stores must conduct store-level staff training and roll out the new system (from initial pilot programs to taking the entire system live).

All in all, under a best-case scenario, it can take merchants a full year—working after hours to avoid inconveniencing customers—to install and operate new EMV terminals. And a lot of small businesses are not facing the best-case scenario with respect to this transition. The card companies’ certification requirements are especially problematic because there is a shortage in the industry of trained personnel capable of conducting the certifications. Even large retailers are experiencing severe delays because of this capacity shortage. Small businesses, despite their best efforts to meet the deadline, are at the back of the line and are having to wait even longer—years in some cases—to complete the EMV transition process.

The U.S., with over 12 million payment terminals and about 1.2 billion cards, is the largest single-market deployment of EMV to date. It is no small undertaking. Notably, banks have been given additional time to get their ATMs EMV-ready; a full *two years* longer, in fact, than merchants have received. But small businesses have not been extended the same assistance, despite the difficul-

ties—beyond their control—with getting their equipment programmed and certified.³

III. Fraud prevention benefits are lost without an accompanying PIN requirement.

Not only is the transition process expensive and onerous for small business owners, but businesses and consumers will not even get full fraud-prevention benefits from it. Making every card PIN-enabled and allowing merchants to require a PIN on their transactions would substantially reduce fraud. Statements Visa and MasterCard have made in other countries suggest they *agree* with that assessment. Merchants are truly dedicated to effective fraud prevention because they pay the bulk of costs associated with card fraud. The card networks, on the other hand, are standing in the way of achieving maximum fraud reduction in the payment card system. Perhaps this should not be a surprise given that those networks do not shoulder any of the losses from fraudulent transactions.

A. Using PIN is the best way to reduce fraud.

Today, the U.S. card payment system is a fraud magnet. Even though the U.S. market accounts for about one quarter of global card volume, almost half of all global credit card fraud occurs in the U.S. Allowing merchants to require PIN numbers for their transactions would dramatically help this situation.

According to the Federal Reserve Board, PIN authentication is *six times* more secure than signature authentication.⁴ When a PIN is required, it protects against fraud in instances where a card number or the card itself is stolen. Chip without PIN, on the other hand, cannot do anything to prevent fraud on stolen cards or prevent online fraud with stolen card numbers. And, chip without PIN may not do much of anything to protect against fraud when card numbers are stolen—which is supposed to be the benefit of the chip. That is because all chip cards will still have a magnetic stripe and a static account number. Fraudsters know they can make a fake card with a fake (non-functioning) chip and it will get run through the magstripe reader as a back-up when the “chip” doesn’t work. So, for chip-without-PIN cards, we remain exposed to all forms of fraud.

Chip and PIN authentication, on the other hand, has a proven track record of significantly decreasing fraud. In fact, Visa advertises these benefits on its own website, noting that in the United Kingdom, fraud related to lost and stolen payment cards has de-

³It is little wonder that this process entails substantial costs and unreasonable timeliness for retailers. The transition process has been dictated entirely by the card companies without input from businesses, consumers, or even banks. In Canada, by contrast, the process of transitioning to EMV had broad stakeholder participation throughout. Their transition to EMV, which was first announced in 2003 (as opposed to 2011 in the U.S.), took 10 years to deploy, even though Canada’s network is 1/10th the size of the U.S. network.

⁴Federal Reserve Board, Debit Card Interchange Fees and Routing, 77 Fed. Reg. at 46,261 (Aug. 3, 2010), available at <http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf>.

creased by more than half since chip and PIN was adopted there in 2004.⁵

Chip without PIN will enable fraud perpetrators to easily shift targets. According to a recent article in the *Washington Post*, “security experts say they widely expect credit card fraud to move online, where thieves can still use the card number and expiration date to make fraudulent purchase.”⁶ Requiring a PIN, however, would address that scenario. And despite card companies’ claims to the contrary, PINs can be—and already are—used online.

In sum, there is simply no legitimate reason for the card companies to move toward a PIN-less path when PIN (with or without a chip) has proven so effective at reducing fraud.

B. Visa and MasterCard agree that PIN increases transaction security

In 2013, Visa and MasterCard jointly petitioned the Australian Competition and Consumer Commission for authorization to *require* PIN authentication on transactions involving their cards.⁷ In their application, they made numerous statements in support of requiring PIN at the point of sale, including:

“The Applicants’ view is that chip and PIN is a significantly more secure form of [customer verification method] than signature.”

“Based on the experience of the introduction of mandatory PIN@[Point of Sale] in overseas markets (in the UK, Canada, Europe and elsewhere), the Applicants expect that certain types of card present fraud will decline in Australia as a result of the introduction of mandatory PIN@POS in Australia.”

“The Applicants note that overseas experience has shown that fraud will move to jurisdictions where there are lower security measures in place and in particular jurisdictions that do not use EMV and PIN security. For example, the UK experience has been that the countries where fraud on UK-issued cards occurs has changed with fraudsters focusing on countries without ‘chip and PIN,’ such as the United States. There has been a similar experience in Europe. Card fraud is highly mobile and is often internationally organized. The coordinated introduction of mandatory PIN@POS in Australia will increase card security in Australia and make it a less attractive jurisdiction for fraudsters.”

⁵ *The Benefits of Chip and PIN for Merchants*, available at <http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp> (last visited Sept. 21, 2015).

⁶ Marte, Jonnelle, *Get Ready to Dip, Not Swipe, Your Credit Cards*, *Washington Post* (Sept. 30, 2015), available at <http://www.washingtonpost.com/news/get-there/wp/2015/09/30/get-ready-to-dip-not-swipe-your-credit-cards/>.

⁷ See generally, Visa and MasterCard—Authorisations—A91379 & A91380, available at <http://registers.accc.gov.au/content/index.phtml?itemId=1120516>.

*“The Applicants believe that mandatory PIN@POS is an important step in the right direction, in terms of reducing credit card fraud in Australia.”*⁸

Despite their representations to the Australian authorities and their affirmative recognition that the use of PIN does improve transaction security, Visa and MasterCard have declined to advance the use of PIN here in the U.S. Instead, they have opted to incentivize chip-without-PIN cards—a move that simply cannot be justified given their own experience and data.

IV. Merchants are committed to reducing fraud because they pay for most of it.

Unlike the card companies, merchants are 100 percent committed to reducing fraudulent transactions and minimizing fraud losses because they currently bear the brunt of an unsecure payments system. We are not opposed to making investments in *effective* security measures. Unfortunately, this very costly transition to EMV will not reduce fraud nearly as much as it could and should, and merchants will not see the relief that they could under a chip and PIN system.

According to an annual report by LexisNexis and Javelin Strategy & Research on the “True Cost of Fraud,” in 2009, retailers suffered fraud losses 10 times higher than financial institutions. The report found that half of retailers’ fraud losses came from unauthorized transactions and card chargebacks—both of which would be significantly reduced by PIN authentication.⁹ The Mercator report has estimated that merchant fraud losses of tens of billions of dollars a year dwarf card-issuer losses.¹⁰ And merchants have no way to remedy this situation. While the card companies give banks the option of requiring PIN at ATMs—and every bank we are aware of does so—they will not allow merchants to do the same. Under the card companies’ operating rules, retailers are prohibited from requiring customers to enter a PIN when accepting debit cards. Ultimately, merchants are at the mercy of the card companies’ policies, which, like this EMV transition, are not designed to maximize consumer protection or card transaction security.

V. Consumers want PIN.

⁸ Submission of Visa Worldwide, Visa AP (Australia), and MasterCard Asia/Pacific to the Australian Competition & Consumer Commission in support of Authorisations A91379 & A91380 (Aug. 30, 2013), “Security of Chip and PIN vs. Signature,” pp. 1-2, available at <http://registers.accc.gov.au/content/index.phtml?itemId=1120516&display=submission> (last visited Sept. 21, 2015).

⁹ Visa recognizes this fact on its Canadian website. In fact, it promotes to retailers:

“Whatever your retail size or specialty, accepting Visa Chip & PIN cards can result in enhanced security and convenience, helping to improve efficiency and reduce the frequency of chargebacks due to fraud. Businesses that accept Chip & PIN cards have benefited from . . . Increased protection against fraud - A PIN is used for cardholder verification and the embedded Chip in the Visa card is virtually impossible to copy. Together these features provide you and your customers with increased protection against fraud, which can result in fewer chargebacks.”

“The Benefits of Chip and PIN for Merchants,” available at <http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp> (last visited Sept. 21, 2015).

¹⁰ Cited in “House of Cards: Why your accounts are vulnerable to thieves,” Consumer Reports, June 2011.

Card companies and banks argue that American consumers do not want PIN. Often, they claim that consumers oppose PIN because consumers will not or cannot remember and use a 4-digit code, or consumers do not want to be inconvenienced by entering a PIN. That argument is belied by consumer research and our everyday experience with ATMs, smart phones, and other devices requiring secure access codes.

In a recent survey commissioned by the National Retail Federation, 62 percent of consumers stated that they would prefer to use chip-and-PIN cards rather than chip-and-signature cards.¹¹ Visa's own statements on this issue are telling. Visa advertises to consumers on its website in Canada (where chip and PIN has been implemented), in a section titled "The Importance of PIN," that "PIN transactions are easy."¹² On the same website, Visa advertises to merchants that businesses that accept chip and PIN cards "have benefited from increased checkout speed and improved customer service—using a PIN is 2 to 4 seconds faster than obtaining a signature"¹³ It is difficult to fathom that the ease and convenience of PIN for consumers and merchants is so much different between Canada and the U.S.

In conclusion, the mandated transition to EMV is flawed in several respects. The transition process, which was developed by the card companies with no other stakeholder input, is very expensive for businesses, contains unreasonable timelines, and is especially difficult for small retailers to implement. To make matters worse, the transition will not achieve the consumer protection and fraud-prevention benefits it easily could. NACS strongly supports effective and meaningful efforts to improve card security, protect consumers, and reduce fraud losses. Unfortunately, this transition is not one of those efforts and it will do more harm than good to small businesses.

¹¹See NRF Survey, available at <https://nrf.com/sites/default/files/Documents/Chip-and-Pin%20Consumer%20Survey%20One-Pager%2009-16-2015%20REV.pdf>.

¹²"The Importance of PIN," available at <http://www.visa.ca/chip/cardholders/importance-of-pin/index.jsp> (last visited Sept. 21, 2015).

¹³"The Benefits of Chip and PIN for Merchants," available at <http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp> (last visited Sept. 21, 2015).



National Grocers Association

U.S. House Small Business Committee
On Behalf of the National Grocers Association
October 6, 2015

The National Grocers Association (NGA) appreciates the opportunity to submit comments for the record to the House Small Business Committee's Subcommittee on Investigations, Oversight and Regulations.

NGA is the national trade association representing the retail and wholesale supermarkets that comprise the independent channel of the food distribution industry. An independent retailer is a privately owned or controlled food retail company operating a variety of formats. Most independent operators are serviced by wholesale distributors, while others may be partially or fully self-distributing. Some independents are publicly traded, but with controlling shares held by the family and others are employee owned. Independents are the true "entrepreneurs" of the grocery industry and dedicated to their customers, associates, and communities. The independent supermarket channel is accountable for close to 1% of the nation's overall economy and is responsible for generating \$131 billion in sales, 944,000 jobs, \$30 billion in wages, and \$27 billion in taxes. Many of our member companies operate on a net profit percentage of 1%, less than most small businesses.

While NGA appreciates the efforts of the Committee to bring attention to the effects of the recent fraud liability shift imposed on small businesses by Visa and MasterCard as part of the migration to chip-enabled payment cards, we are disappointed that no small business merchants are testifying at this important hearing. NGA believes that greater attention must be paid to the challenges that small businesses are currently facing as they strive to implement this new technology, and furthermore, the lack of security that the chip-and-signature technology provides in comparison to the chip-and-PIN (personal identification number) technology that has been employed throughout Europe for more than 20 years.

EMV Background:

EMV stands for Europay, MasterCard and Visa, the founding members of EMVCo in 1994. EMV technology includes payment cards that contain an embedded computer chip that allows for increased security through card validation and cardholder authentication that reduces fraud from lost and stolen cards. EMV technology has been the standard throughout much of the rest of the world for nearly 20

years, though EMV technology abroad has required a PIN (personal identification number) to be entered with each transaction, while U.S. EMV will only require a signature, despite evidence that transactions involving a PIN are far more secure than a signature.

The transition to EMV in the United States began in 2011 when the payment brands introduced a pathway to adoption. The U.S. was scheduled to complete the transition to EMV on October 1, 2015. This transition included the implementation of chip-and-signature technology, requiring all merchants to update their point-of-sale (POS) card terminals in addition to the software that runs the front end systems at an expected cost to merchants of \$30 billion, according to the National Retail Federation. For merchants that fail to meet the deadline for upgrading their POS card readers, the liability for fraud committed in their stores using chip-and-signature cards will shift to the merchant. Throughout this process, merchant input and feedback has been stymied. The payment brands, as represented by EMVCo, have dictated the terms and conditions of the transition from the outset, and have been unresponsive to the needs of merchants who, many through no fault of their own, were not ready for the liability shift on October 1 due to delays in production or certification.

Unfortunately, many NGA members invested tens of thousands or in some instances hundreds of thousands of dollars to upgrade hardware and software only to learn that their systems would not be ready by October 1, 2015 because necessary upstream certifications were severely backlogged. We understand some of the backlog was a result of a delay to provide necessary software code for parties to implement and certify by the deadline. As a result, thousands of independent grocers, including many small businesses, are now subject to this liability shift due to delays that were entirely out of their control. NGA strongly believes this is unacceptable and urges Visa and MasterCard to immediately take steps to ensure these merchants do not face losses as a result of the liability shift.

Though EMV has been the standard for nearly two decades throughout Europe and much of Asia, a more instructive comparison might be the Canadian transition to EMV, which began only a few years ago. Visa was the first company in Canada to announce the conversion to chip-and-PIN in 2003, with other card issuers not far behind. Trials of the technology began in 2007 and lasted through 2009, with the first liability shift not set until October of 2010, a full 7 years after the shift was announced. In addition, the liability shift dates were moved on multiple occasions due to the fact that POS terminals were not available as a result of delays in production, meaning that many larger merchants would be receiving their terminals in the months leading up to the holidays and would be forced to train their staff and customers on a new technology during the busiest time of year for merchants. Visa and MasterCard both changed their liability shift deadlines from October 2010 to March 2011 in order to accommodate these merchants.

Neither Visa nor MasterCard granted an extension of the liability shift in the U.S., despite a timeline that was several years shorter¹.

Challenges to Implementation:

Despite the best efforts of merchants large and small alike, many are facing significant challenges as they seek to implement the new EMV technology at the POS. Due to the sheer volume of terminals that need replacement (more than 12 million²), many stores have faced massive delays in receiving their terminals, in the installation of their terminals, and during the certification process. Many merchants report delays of weeks and even months at each stage of the transition. One NGA member reports that they are still waiting for software to be installed at the POS despite ordering their terminals in April of 2015. In many instances technicians must physically install each PIN pad terminal at checkout lanes. With certification delays, piloting, and staff training, this store will likely be liable for fraudulent purchases for several months, despite beginning the transition more than 6 months in advance of the deadline. Another NGA member operating more than 75 stores, has had their terminals installed in their stores for nearly a year at an expense of more than \$400,000 but has still not been provided with the software needed to certify and activate the terminals. Again, despite beginning the transition process more than a year in advance of the deadline, this company was not EMV compliant on October 1 and will be liable for any fraudulent purchases made with EMV cards until they can be provided with the software to activate their terminals.

Once merchants have received their POS terminals, often after 6-16 weeks of delays, there is still a lengthy process of programming, testing and certification before terminals are ready for customer use. Each of these steps can involve weeks of delays for various reasons. One of the most commonly reported issues facing merchants on their road to implementation is the severe shortage of terminal installation experts, which has led to significant delays in initial installation. A separate certification process for each of the major card brands (Visa, MasterCard, American Express and Discover) further complicates an already daunting process.

Current Standards:

The Payment Card Industry (PCI) data security standard (DSS) is applied to anyone that processes, stores or transmits credit card information-regardless of size. Founded by the five major payment brands (Visa, MasterCard, Discover, American Express and JCB), PCI has the ability to levy fines as high as \$100,000 per month against acquiring banks-with the full expectation that it will be

¹ EMV-USA. EMV Migration-Canada. Tracy Black. 02/15.

² Federal Reserve Bank of Chicago. Kandice Alter and Anna Neumann. 05/18/15.

passed down to the merchant. In addition to passing along fines, it is possible that an acquiring bank could terminate their relationship with the merchant altogether, or increase transaction fees.

PCI standards have been thrust onto merchants large and small without allowing the voice of the merchant to be heard in the process of creating those same standards- nor have merchants been allowed to participate in the PCI executive committee that serves as the main governing body for PCI. For those merchants unfortunate enough to suffer a data breach that results in the loss of sensitive consumer data, it is likely that PCI will find the merchant to be out of compliance with the PCI DSS and will levy fines, despite the fact that the merchant had been certified as PCI compliant prior to the breach. For small businesses, this can be disastrous. According to the National Cyber Security Alliance, 60% of all small businesses that suffer a data breach will go out of business within six months.

More Security Needed:

As an integral part of the community that many customers visit more than once a week, supermarkets are fully committed to protecting their customers' personal information. NGA members continue to go above and beyond current security requirements such as PCI standards, by investing millions of dollars towards instituting end-to-end encryption, tokenization, and further exploring current best practices and emerging technologies that will allow them to better safeguard customer data. Unfortunately, card-issuing banks have chosen not to implement the full use of chip-and-PIN technology in the United States, instead opting for the less-secure chip-and-signature. According to the United States Federal Reserve, chip-and-PIN technology is more than 700%³ more secure than chip-and-signature-and yet banks have chosen a half-measure move to chip-and-signature at the expense of the merchant.

According to a recent survey conducted by the National Retail Federation, 62% of consumers would prefer to be issued chip-and-PIN cards, and 63% believe that chip-and-PIN provides more security than simple chip-and-signature⁴. Unfortunately, card-issuing banks have opted for the more fraud-prone signature option, putting customers' data and businesses at risk. While banks contend that consumers would balk at the idea of having to remember another PIN number, NRF's survey indicated that 83% of consumers would consider it worthwhile to remember another PIN in exchange for greater security. Despite consumer and merchant interest in chip-and-PIN technology, card-issuing banks have opted for less security-putting consumers and merchants at risk.

High-profile breaches in the last few years have greatly increased the level of awareness for the public and merchant community alike with regard to payment security, as the cost of fraud has

³ "2011 Interchange Fee Revenue, Covered Issuer Costs, And Covered Issuer And Merchant Fraud Losses Related To Debit Card Transactions," 3/5/13

⁴ Chip-and-PIN Consumer Survey One-Pager. 09/16/15.

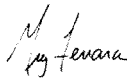
skyrocketed from \$23 billion in 2013 to \$32 billion in 2014⁵. While the U.S. has seen its incidents of fraud increase, Canada saw its fraud reduced by 40% from 2011-2012 once chip-and-PIN was instituted⁶, while the EU has seen an 80% reduction in fraud since its transition to chip-and-PIN EMV⁷. With a proven track record of preventing fraud in multiple regions throughout the globe, there is little reason to not institute chip-and-PIN in the U.S.

NGA Position:

The National Grocers Association (NGA) fully supports all efforts to make the payments chain more secure. NGA believes that all members of the payment chain should make use of every available technology in order to protect consumer information. NGA supports the implementation of chip-and-PIN technology, tokenization, end to end encryption, and other advanced security measures that would better ensure that consumer information remains safe throughout the payment chain.

We look forward to continuing a constructive dialog with the Committee on these issues and others important to the independent supermarket channel, and are hopeful that the merchant community will have the same opportunity to present the challenges they are experiencing in front of the Committee at another EMV hearing in the near future. Thank you for the opportunity to submit these comments.

Sincerely,



Greg Ferrara
Vice President, Public Affairs
National Grocers Association

⁵ Reuters. \$32 Billion Lost by Retailers to Credit Card Fraud—SmartMetric Brings Biometric Technology to Credit Card. 02/17/15.

⁶ Chase Paymentech Solutions. 2012.

⁷ Discover Financial Services. 2013.



Submission for the Record
to the
Small Business Committee
of the
U.S. House of Representatives
on behalf of
The National Retail Federation
for the
Hearing on “The EMV Deadline and What it Means for Small Businesses”

David French
Senior Vice President,
Government Relations
National Retail Federation
202.626.8112
frenchd@nrf.com

NATIONAL RETAIL FEDERATION
1101 New York Avenue, NW, Suite 1200
Washington, DC 20005
www.nrf.com

The EMV Deadline and What It Means for Small Businesses
Statement of the National Retail Federation
October 7, 2015

The National Retail Federation submits this statement for the record with respect to the House Small Business Committee October 7, 2015 hearing regarding the “EMV Deadline and What it Means for Small Businesses.” By way of background, the National Retail Federation is the world’s largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation’s largest private sector employers, supporting one in four U.S. jobs—42 million working Americans. Contributing \$2.6 trillion to annual GDP, retail is a daily barometer for the nation’s economy. NRF’s *This is Retail* campaign highlights the industry’s opportunities for life-long careers, how retailers strengthen communities, and the critical role that retail plays in driving innovation. Thousands of our retail members, and millions of merchants of all types, whether small retailers or other operations, such as doctors’ offices, tax drivers, or dry cleaners, will be affected by the subject of the hearing.

It is important to note at the outset that the EMV deadline at issue is neither legislatively established, nor is it in fact a true deadline. Rather, it is an arbitrary date, imposed by a consortium of card companies and banks who have, for many years, collectively exerted near monopoly power over the business community. This “deadline” is for the financial benefit and convenience of those companies and banks. The relationship between those powerful entities and small businesses is purely contractual; albeit largely compulsory in effect, since retailers and other small businesses are subject to the substantial combined market power of the financial institutions.

A second important note is that the standard in question, EMV, is purely a propriety technology of the largest card companies and banks. EMV Co. is essentially the creation of MasterCard and Visa. Visa and MasterCard in turn are the collective creations of the thousands of banks and credit unions who formed them, originally as trade associations, to advance their card products and other interests. When Visa and MasterCard set suggested fees that businesses must remit from their gross sales to financial institutions, with virtually no exceptions, every bank and credit union simultaneously imposes those fees. There is no competition. And the fees are very high. For many small businesses, card fees are their second largest expense after labor.

These collective entities also impose a multitude of complex rules on small businesses. The rules govern not only what business may say or do in their stores and at their cash registers, but also dictate steps that businesses may or may not take to prevent fraud. It has been known for several years that the cards U.S. consumers carry

in their wallets are fraud-prone. The rules ensure that businesses, not the card-issuing banks, pay for the majority of that fraud. For example, businesses are either primarily or totally responsible for disputed transaction fraud and Card-Not-Present fraud (such as Internet transactions), among other categories. The financial institutions are responsible, in some instances, for authenticating their cards. But beyond those limited circumstances the burden of fraud has been shifted by card company rules onto businesses. What's more, businesses are told they must pay for fraud "up front" in the form of ever rising swipe fee for the privilege of accepting cards.

Secure, PIN-protected cards (computer chips were primarily added for other purposes) were long ago introduced in Europe and elsewhere to combat fraud; however, the card issuing collective rejected both measures in the U.S. for two decades. So long as fraud was effectively being absorbed by small businesses and others, it apparently was not a serious concern of the card issuing consortium. The sensitive card numbers remained exposed, not only on the magnetic stripe, but embossed on the face of the card itself. Nearly a decade ago, NRF strongly encouraged the card industry to remove the raw card numbers from common circulation. The card industry rejected that suggestion.

Rather than jointly work with the businesses community to encrypt or tokenize card numbers and thus make them less valuable to thieves, the card companies instead created yet another entity (PCI Co.) to impose additional rules on business of all sizes. It basically demanded that everyone attempt to build even higher walls within their systems to "protect" the card companies' numbers. Of course, if one builds eight foot walls, cyber thieves will bring ten foot ladders. And they did. Aided by ever more powerful computers, hacks on processors, banks, merchants and networks escalated.

Fraud has increased. The type of fraud for which banks are initially responsible has also increased. Consequently, they and the card companies have belatedly sought to introduce into the U.S. cards that would reduce fraud, much as they did in Europe and Canada years ago. But they have ignored the lessons of those countries. Rather than introduce U.S. cards with PINs (which reduce all types of fraud), abetted by Chips (which help reduce just in-store, counterfeit fraud), they are introducing Chip without PIN cards; i.e. partially protective cards.

In turn, the card industry is demanding that the entire merchant community spend between \$30 and \$35 billion dollars to install Chip and PIN terminals, but, with precious few exceptions, banks are only willing to undertake the expense of introducing Chip *without* PIN cards. These new cards do not reduce fraud across the board. They only reduce the particular type of fraud for which the banks are primarily responsible. Installation costs vary dramatically, from a few hundred dollars to thousands of dollars per terminal. The only "incentive" merchants are given to purchase and install the expensive new systems is the threat that merchants will be forced to absorb not only the fraud banks already make businesses shoulder, but also to pay the full measure of the banks'

fraud exposure if small businesses do not comply with the consortium's mandate.

While the new cards make it somewhat more difficult for criminals to use stolen card numbers, they do not actually prevent numbers from being stolen in the first place, and stolen numbers can still be used for online and other types of fraud.

The new EMV equipment does not stop breaches. Indeed, in many cases it provides no significant benefits either to the business or to the business' regular customers. It is merely an additional expense small businesses are being told to bear as part of the card companies' efforts to extend their growing monopoly over the payment system. If businesses can be forced to quickly install, at significant expense, the kinds of equipment that is most compatible with EMV Co.'s and the card companies' future business plans (EMV Card Personalization; Chip-based contact specifications—near field communications technology, etc.) then competitive alternatives, such as new mobile platforms (e.g. Starbucks-style payment programs) may effectively be locked out of the market.

These are important considerations that businesses of all sizes must carefully ponder. It would be inappropriate to prejudge their decision-making and stampede businesses into the adoption of solutions less protective for businesses and consumers than has existed throughout the industrialized world for more than a generation.

